A NON-DETERMINISTIC PUBLIC KEY ENCRYPTION SYSTEM

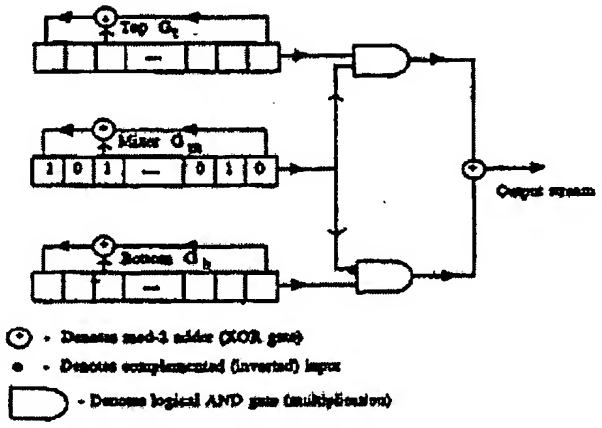
Patent number: WO9515633
Publication date: 1995-06-08
Inventor: RAIKE WILLIAM MICHAEL [NZ]
Applicant: RAIKE WILLIAM MICHAEL [NZ]
Classification:
- international: H04L9/30; H04L9/32; H04L9/06; H04L9/24; H04L9/00
- european: H04L9/08; H04L9/22; H04L9/30; H04L9/32
Application number: WO1994NZ00136 19941201
Priority number(s): NZ19930250337 19931201; NZ19930250475 19931216; NZ19940260712 19940609

Also published as:
EP0734624 (A1)
US5799088 (A1)
JP2002314534 (A)
AU702766 (B2)

Cited documents:
US4165444
EP0325238

Abstract of **WO9515633**

A non-deterministic public key encryption system whereby a public key is generated from a private key using mathematical operations equivalent to exponentiation in finite fields. Thus an attacker is required to compute logarithms over finite fields. Encryption involves generating a random initialisation key (R) which is used to (1) exponentiate the message receiver's public key (E) to produce initial values (K) for a pseudorandom binary mixture generator, and to (2) compute an open key (Q) by exponentiating an initial known generator state (a0). A ciphertext (C) is produced from plaintext (P) by clocking the mixture generator from the initial value (K) and combining the output keystream with the plaintext (P). The open key (Q) is attached to the ciphertext prior to transmission. Decryption involves extracting the open key (Q) and exponentiating this by the message receiver's private key (D) to compute (K) which is then used to set the initial value of a mixture generator. The mixture generator is clocked and its output keystream combined with the ciphertext (C) to produce plaintext (P). The invention may be implemented in special purpose hardware or in software for a general purpose processor.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平9－509748

(43)公表日　平成９年(1997)９月30日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ｄ
		６２０	7259－5Ｊ			６２０Ａ
		６４０	7259－5Ｊ			６４０Ｂ
Ｈ０４Ｌ	9/24		9570－5Ｊ	Ｈ０４Ｌ	9/00	６５７
	9/30		9570－5Ｊ			６６３Ａ

審査請求　未請求　　予備審査請求　有　　（全 76 頁）　最終頁に続く

(21)出願番号　特願平7－515543
(86)(22)出願日　平成６年(1994)12月１日
(85)翻訳文提出日　平成８年(1996)５月31日
(86)国際出願番号　ＰＣＴ／ＮＺ９４／００１３６
(87)国際公開番号　ＷＯ９５／１５６３３
(87)国際公開日　平成７年(1995)６月８日
(31)優先権主張番号　２５０３３７
(32)優先日　1993年12月１日
(33)優先権主張国　ニュー・ジーランド（ＮＺ）
(31)優先権主張番号　２５０４７５
(32)優先日　1993年12月16日
(33)優先権主張国　ニュー・ジーランド（ＮＺ）

(71)出願人　ライク，ウイリアム，マイケル
ニュージーランド国オークランド，スワンソン，シンプソン　ロード　66
(72)発明者　ライク，ウイリアム，マイケル
ニュージーランド国オークランド，スワンソン，シンプソン　ロード　66
(74)代理人　弁理士　浅村　皓　（外３名）

最終頁に続く

(54)【発明の名称】　非決定論的公開キー暗号化システム

(57)【要約】
有限場における累乗に等価的な数学的演算を用いて、プライベートキーから公開キーを発生する非決定論的公開キー暗号システムである。従って、侵入者は有限場の対数を計算しなければならない。暗号化を行うにはランダム初期化キー（Ｒ）を発生する。このランダム初期化キー（Ｒ）は疑似ランダム二進ミクスチャー発生器に対する初期値（Ｋ）を発生するよう、メッセージの受信者の公開キー（Ｅ）を累乗（１）し、更に初期の公知の発生器のステート（ａ０）を累乗することにより、オープンキー（Ｑ）を計算（２）するのに使用される。初期値Ｋからミクスチャー発生器をクロック制御し、出力キーストリームと平文Ｐとを組み合わせることにより平文Ｐから暗号文Ｃを発生する。送信前に暗号文にオープンキー（Ｑ）を添える。暗号解読を行うにはオープンキー（Ｑ）を抽出し、これをメッセージ受信者のプライベートキー（Ｄ）で累乗して、ミクスチャー発生器の初期値をセットするのに使用される（Ｋ）を計算する。ミクスチャー発生器をクロック制御し、その出力キーストリームと暗号文（Ｃ）とを組み合わせ、平文（Ｐ）を発生す

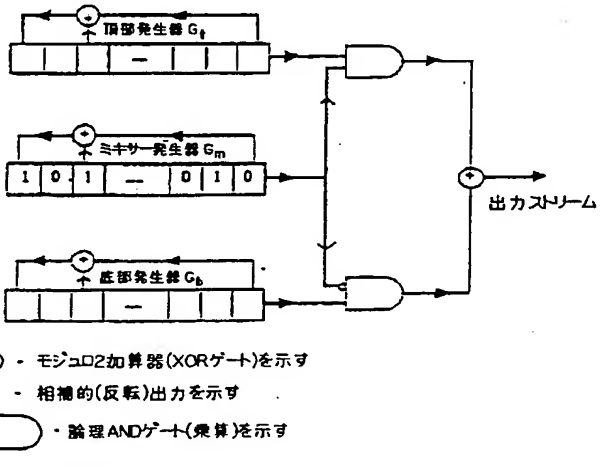


FIG 2

【特許請求の範囲】

１．メッセージ発信者がメッセージ受信者に固有の公知のキーを使って平文メッセージＰを暗号化し、メッセージ受信者が公開キーを発生した秘密のプライベートキーを使用して暗号化メッセージを暗号解読する公開キー暗号システムにおいて、

（１）複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、

（２）前記数$D_{1\sim n}$の各々に対してプライベートキー$D_{1\sim n}$によって得られた対応する数に等しい数のクロックパルスまたはステート変化の後に所定の公知の初期ステートから疑似ランダム二進数発生器のステートを発生し、公開キー（Ｅ）の成分として計算された二進ステート$E_{1\sim n}$の各々を提供することによりプライベートキーを用いて（先に記載した）累乗により公開キー（Ｅ）を計算し、

（３）メッセージ発信者が、

（ａ）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を発生し、数$R_{1\sim n}$の各々に対してランダム初期化キー$R_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の公知の初期ステートから疑似ランダム二進数発生器のステートを計算し、オープンキーＱの成分として計算された二進数ステート$O_{1\sim n}$を提供することにより、累乗によりオープンキーＱを計算し、

（ｂ）公開キー$E_{1\sim n}$の成分をランダム初期化キー$R_{1\sim n}$の成分により累乗し、前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対し、工程（２）に記載の方法を対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じた疑似ランダム二進数発生器のステートを計算することにより、発生器初期化ステート$K_{1\sim n}$を発生し、

（ｃ）第１ミクスチャー発生器を形成するように出力が組み合わされている一組（ｎ）の疑似ランダム二進数発生器に初期値$K_{1\sim n}$をロードし、

（ｄ）キーストリームシリアル出力を得るように、第１ミクスチャー発生器をクロックし、

（ｅ）前記キーストリーム出力と二進平文メッセージＰとを組み合わせて暗号化されたビットストリーム暗号文Ｃを発生し、

（ｆ）暗号文Ｃをオープンキー Ｑに加え、メッセージストリームを発生し、

（ｇ）メッセージをメッセージ受信者に送信し、

（４）メッセージ受信者が、

（ａ）メッセージストリームからオープンキー Ｑを抽出し、

（ｂ）ステップ（３）（ａ）に記載の方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することにより得られる疑似ランダム二進数派生機のステートを、前記数$Q_{1\sim n}$および$D_{1\sim n}$の各々に対して計算することにより、発生器初期化ステート$K_{1\sim n}$を発生するようにオープンキー Ｑをプライベートキー Ｄで累乗し、

（ｃ）ミクスチャー発生器を形成するように出力が組み合わされた第２の組（ｎ）の疑似ランダム二進数発生器に発生器初期化ステート$K_{1\sim n}$をロードし、

（ｄ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力と受信した暗号化ビットストリームとを組み合わせて発信者の平文メッセージを発生することを特徴とする、公開キー暗号システム。

２．前記ミクスチャー発生器が一組（ｎ）の最大期間線形シフトレジスタ発生器を備え、すべての発生器がクロック制御される際に前記キーストリームシリアル出力を発生するよう、組内の１つの発生器が他（ｎ－１）の発生器の出力をメモリレス状に選択するようになっている、請求項１記載の公開キー暗号システム。

３．前記ランダム初期化キー Ｒを発生することが、

（１）ある時間ｔにおけるステートが複数の座標（X_{t1}、X_{t2}、....、X_{tn}）によって示された点X_tとして表示できる電子ポインタデバイスを操作する工程と、

（２）複数の時間ｔ＝１、２、....、ｎにおける前記入力デバイスのステートを表示する点X_tを測定する工程と、

（３）前記時間のサブセットに対応する、上記のように測定された点のサブセットを選択する工程と、

（４）このように選択された点すべての座標の数値関数を計算する工程と、

（５）このように計算された数値関数の値を示す複数の二進数として、所望の乱数を発生する工程とを備えた、請求項１記載の公開キー暗号システム。

４．前記暗号文Ｃを発生するように前記キーストリームと二進平文Ｐとを組み合わせる工程が、Ｐの各成分P_iに対し、

（１）シリアルキーストリームの出力の複数のバイトを使用して、バイト１、...、ｎ　の疑似ランダム順列Ｔを発生する工程と、

（２）中間部分I_iを形成するよう順列Ｔに従って部分P_i内にバイトn_iの相対位置を順列する工程と、

（３）中間部分I_iの各バイトに対し、

（ａ）シリアルキーストリーム出力の１つ以上のバイトを発生し、

（ｂ）バイトＢおよびシリアルキー出力の前記発生されたバイトに応じた値と置換することにより暗号化されたビットストリームのｉ番目の部分C_iを形成する工程とを備えた、請求項１～３のいずれかに記載の公開キー暗号システム。

５．連続する各部分P_iに対して開始点からP_iまで（P_iを含む）の二進情報Ｐのすべての部分に対する累算的な現在メッセージダイジェスト値D_iを計算する工程と、現在のメッセージダイジェスト値D_iに依存する数の付加的バイトのシリアルキーストリーム出力を得てこれを廃棄する工程を更に含む、請求項４記載の公開キー暗号システム。

６．複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、前記数$D_{1\sim n}$の各々に対しプライベートキー$D_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$E_{1\sim n}$の各々を公開キーＥの成分として提供することにより、プライベートキーを使用して公開キー（Ｅ）を累乗する、公開キー暗号システム用の暗号化装置であって、

一組の二進数$R_{1\sim n}$を備えたランダム初期化キー（Ｒ）を発生するための手段と、

前記数$R_{1\sim n}$の各々に対しランダム初期化キーR$_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変換の後に、所定の公知の初期ステートから疑似ランダム二進数発生器のステートを計算することにより、累乗によりオープンキーQを計算するための手段と、

前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対し、公開キーEを累乗するのに使用される方法を対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似

ランダム二進数発生器のステートを計算することにより、発生器の初期化ステートK$_{1\sim n}$を発生するよう、公開キーEの成分をランダム初期化キーRの成分で累乗するための手段と、

ミクスチャー発生器の出力を形成するように出力が組み合わされた一組（ｎ）の疑似ランダム二進数発生器を含むミクスチャー発生器と、

前記組（ｎ）の疑似ランダム二進数発生器にK$_{1\sim n}$に等しい初期値をロードする手段と、

キーストリームシリアル出力を得るようにミクスチャー発生器をクロック化する手段と、

平文メッセージを受信し、ミクスチャー発生器の出力と二進平文メッセージとを組み合わせ、暗号化されたビットストリームを発生する手段と、

暗号文Cをオープンキー Qに加え、メッセージストリームを発生する手段と、

メッセージストリームをメッセージ受信者に送信するための手段とを備えた、公開キー暗号システムのための暗号化装置。

７．複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、前記数$D_{1\sim n}$の各々に対しプライベートキーD$_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算した二進ステート$E_{1\sim n}$の各々を公開キー（Ｅ）の成分として提供することにより、プライベートキーを使用して公開キー（Ｅ）を累乗し、

メッセージ発信者が、

（１）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を発生し、前記数$R_{1\sim n}$の各々に対しランダム初期化キー$R_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の公知の初期ステートから疑似ランダム二進数発生器のステートを計算し、オープンキーＱの成分として計算された二進数ステート$Q_{1\sim n}$を提供することにより、累乗によりオープンキーＱを計算し、

（２）公開キーＥの成分をランダム初期化キーＲの成分により累乗し、プライベートキーを用いて公開キーを累乗すると先に定義した方法を、対応する二進数

$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似ランダム二進数発生器のステートを前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対して計算することにより、発生器初期化ステート$K_{1\sim n}$を発生し、

（３）第１ミクスチャー発生器を形成するように出力が組み合わされている疑似ランダム二進数発生器の組（ｎ）に初期値$K_{1\sim n}$をロードし、

（４）キーストリームシリアル出力を得るように、第１ミクスチャー発生器をクロックし、この出力と二進平文メッセージとを組み合わせて暗号化されたビットストリーム暗号文Ｃを発生し、

（５）オープンキーＱとともに、暗号化されたビットストリームをメッセージ受信者に送信するような方法に従って平文メッセージを暗号化し、

暗号解読装置が、

暗号化されたビットストリームからオープンキーＱを抽出するための手段と、

オープンキーＱを発生するよう、上記記載の方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することにより生じた疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するようプライベートキーＤの成分によりオープンキーＱの成分を累乗するための手段と、

ミクスチャー発生器を形成するよう出力が組み合わされた一組（ｎ）の疑似ランダム二進数発生器と、

前記組（ｎ）の疑似ランダム二進数発生器に$K_{1\sim n}$に等しい初期値をロードする手段と、

キーストリームシリアル出力を得るよう、ミクスチャー発生器をクロック制御するための手段と、

この出力と受信された暗号文Ｃとを組み合わせて平文メッセージＰを発生するための手段とを備えた、公開キー暗号システムのための暗号解読装置。

８．メッセージ発信者がメッセージにサイン情報を添え、公衆が検査できるようにオープンにされたサインアーカイブに発信者の名前と共に対応する認証情報を登録し、メッセージ証明者がメッセージおよびそのサイン情報、更に公共サインアーカイブからの認証情報を得て、これらを使って前記サイン情報によって識別された発信者によりメッセージが送られたものであるかどうかを確認する、公開キー認証システムにおいて、

（１）メッセージ発信者が、

（ａ）複数の二進数$S_{1\sim n}$から成るランダムデジタルサイン（Ｓ）を選択し、

（ｂ）前記数$S_{1\sim n}$の各々に対しランダムデジタルサイン$S_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$V_{1\sim n}$の各々を証明キーＶの成分として提供することにより、証明キーＶを累乗し、

（ｃ）工程（ｂ）において計算された証明キーＶがまだ登録されたものでないかどうか確認するよう前記サインアーカイブをチェックし、先に登録されたものであれば工程（ａ）、（ｂ）を繰り返し、

（ｄ）一組（ｎ）の疑似ランダム二進数発生器のうちの各々に対して、送信されたメッセージを含むビットシーケンスを前記ランダム二進数発生器に対応する法で割ることによって得られる剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チェック（ＣＲＣ）値Ｃの成分として提供することにより、ＣＲＣ値Ｃを計算し、

（ｅ）合計Ｃ＋Ｓ（モジュロ２）を計算し、公共サインアーカイブ内にメッセージ送信者の名前でこの合計および証明キーＶを登録し、

（ｆ）Ｓを送信メッセージに添え、

（２）メッセージ証明者が、

（ａ）メッセージから複数の二進数$S_{1\sim n}$を備えたデジタルサイン（Ｓ）を抽出し、

（ｂ）前記数$S_{1\sim n}$の各々に対して、受信したメッセージを含むビットシーケンスを疑似ランダム二進数発生器に対応する法で割ることによって得られる剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チェック（ＣＲＣ）値Ｃの成分として提供することにより、ＣＲＣ値Ｃを計算し、

（ｃ）前記数$S_{1\sim n}$の各々に対し工程（１）（ｂ）に記載された方法により前記各数$S_{1\sim n}$を使用して対応する疑似ランダム二進数発生器の所定初期値を累乗することにより証明キーＶを計算し、

（ｄ）合計Ｃ＋Ｓ（モジュロ２）を計算し、

（ｅ）値Ｃ＋Ｓ（モジュロ２）と工程（ｃ）および（ｄ）で計算されたＶが一致する認証情報を探すよう、メッセージのうちの前記サイン情報によって識別される発信者の名前で公共サインアーカイブをサーチし、

（ｆ）工程（Ｅ）におけるサーチが成功した場合、メッセージを正しいものと認め、または工程（ｅ）におけるサーチが成功しなかった場合、メッセージを偽物として拒否することを特徴とする、公開キー認証システム。

９．メッセージ認証者が複数の二進数$D_{1\sim n}$を含むプライベートキーＤを選択し、前記数$D_{1\sim n}$の各々に対しプライベートキー$D_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定初期ステートから疑似ランダム二進数発生器のステートを計算し、計算した二進ステート$E_{1\sim n}$の各々を公開キーＥの成分として提供することにより、プライベートキーを用いて公開キーＥを累乗し、公開キーを公衆の検査ができるようにし、メッセージ発信人が前記メッセージ認証者と共に固有の認証情報を登録し、メッセージにサイン情報を添え、メッセージ証明者がメッセージを得て、メッセージのための一般化されたＣＲＣ値を計算し、メッセージサイン情報、一般化されたＣＲＣ値および発信者の名前またはその他の識別情報をメッセージ認定者へ送り、前記メ

ッセージ認証者が前記一般化されたＣＲＣ値、前記メッセージサイン情報および前記登録された認証情報を使用して、メッセージが前記認証情報によって識別された発信者によって送信されたものであるかどうかを確認する、公開キー認証システムにおいて、

（１）メッセージ発信者が、

（ａ）複数の二進数から成る認証パスワード（Ｐ）を選択し、

（ｂ）認証パスワードＰを登録し、発信者の名前または他の識別情報に対応させ、Ｐが他人によって登録されていないかどうかを確認することを前記サイン認証者に求め、Ｐがすでに登録されていると通知を受けた場合、工程（ａ）を繰り返し、

（ｃ）一組（ｎ）の疑似ランダム二進数発生器の各１つに対し、送信メッセージを含むビットシーケンスを前記疑似ランダム二進数発生器に対応する法で割ることにより得られた剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チェック（ＣＲＣ）値C_Mとして提供することにより、一般化されたＣＲＣ値C_Mを計算し、

（ｄ）一般化されたＣＲＣ値C_Mを認証パスワードＰに添えることにより中間サイン情報を計算し、

（ｅ）（ｉ）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を選択し、前記数$R_{1\sim n}$の各々に対し、ランダム初期化キー$R_{1\sim n}$によって示される数のクロックパルスまたはステート変化の後に所定の初期値から疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$Q_{1\sim n}$の各々を提供して、オープンキーＱを発生することにより各数を用いて初期値を累乗し、

（ｉｉ）前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対しプライベートキーを用いて公開キーを累乗すると先に記載した方法を、対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するよう、サイン認証公開キーＥの成分をランダム初期化キーＲの成分で累乗し、

（ｉｉｉ）ミクスチャー発生器を形成するように出力が組み合わさ

れた一組（ｎ）の疑似ランダム二進数発生器に初期値$K_{1\sim n}$をロードし、

（ｉｖ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力と前記中間サイン情報とを組み合わせ、暗号化された中間サイン情報を発生し、

（ｖ）該暗号化された中間サイン情報を前記オープンキーＱに添えてメッセージサイン情報$S_{P,M}$を発生することによってサイン認証公開キーＥを使って工程（ｄ）で計算された中間サイン情報を暗号化することによりメッセージサイン情報$S_{P,M}$を計算し、

（ｆ）該メッセージサイン情報$S_{P,M}$をメッセージに添え、更に発信者の名前またはその他の識別情報をメッセージに添え、

（２）メッセージ証明者が、

（ａ）メッセージからメッセージサイン情報（$S_{P,M}$）および発信者の名前または他の識別情報を抽出し、

（ｂ）工程（１）（ｃ）に記載された方法によりメッセージに対する一般化されたＣＲＣ値C_M'を計算し、

（ｃ）該メッセージサイン情報、発信者の名前、または他の識別情報および前記一般化されたＣＲＣ値C_M'をサイン認証者へ送り、該サイン認証者にメッセージサイン情報$S_{P,M}$内の暗号化された認証パスワードＰおよび一般化されたＣＲＣ値C_Mと、C_M'および発信者の名前または他の識別情報とを比較することを求め、

（３）メッセージ認証者が、

（ａ）（ｉ）メッセージサイン情報からオープンキーＱを抽出し、

（ｉｉ）前記数$Q_{1\sim n}$および$D_{1\sim n}$の各々に対し工程（１）（ｅ）（ｉ）に記載された方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することによって得られる疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するよう、オープンキーＱをプライベートキーＤで累乗し、

（ｉｉｉ）ミクスチャー発生器を形成するように出力が組み合わされた第２の組（ｎ）の疑似ランダム二進数発生器に発生器の初期化ステートＫ$_{1\sim n}$をロードし、

（ｉｖ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力とメッセージサイン情報とを組み合わせて工程（１）（ｄ）で計算された中間サイン情報ＰおよびＣを再現することにより、プライベートキーＤを用いてメッセージサイン情報Ｓ$_{P,M}$を暗号解読し、

（ｂ）前記中間サイン情報に含まれたＰの値と、工程（２）（ｃ）で送られた名前または他の識別情報に対応して登録された認証パスワードとを比較し、

（ｃ）前記中間サイン情報に含まれたＣ$_{M}$の値と、工程（２）（ｃ）で送られたＣ$'_{M}$の値とを比較し、

（ｄ）工程（ｃ）および（ｄ）における双方の比較に成功した場合、メッセージが正しいものであることをメッセージ証明者に確認し、いずれかの比較に失敗した場合、偽物としてメッセージを拒否することを特徴とする、公開キー認証システム。

１０．（１）ある時間ｔにおけるステートが複数の座標（Ｘ$_{t1}$、Ｘ$_{t2}$、．．．．、Ｘ$_{tn}$）によって示された点Ｘ$_{t}$として表示できる電子ポインタデバイスを操作する工程と、

（２）複数の時間ｔ＝１、２、．．．．、ｎにおける前記入力デバイスのステートを表示する点Ｘ$_{t}$を測定する工程と、

（３）前記時間のサブセットに対応する、上記のように測定された点のサブセットを選択する工程と、

（４）このように選択された点すべての座標の数値関数を計算する工程と、

（５）このように計算された数値関数の値を示す複数の二進数として、所望の乱数を発生する工程とを備えた、乱数を発生するための方法。

１１．一連の部分Ｃ$_{j}$を含む暗号化されたビットストリームＣを発生するよう、各部分Ｐ$_{j}$が多数のバイトｎ$_{j}$を示す一連の部分Ｐ$_{1}$、．．．．、Ｐ$_{N}$を備えた二進情報Ｐとシリアルキーストリーム出力とを組み合わせる方法であって、

（１）シリアルキーストリーム出力の複数のバイトを使用してバイト１、....、n_iの疑似ランダム順列Ｔを発生する工程と、

（２）中間部分I_iを形成するよう、順列Ｔに従って部分P_i内のバイトn_iの相対位置を順列する工程と、

（３）中間部分I_iの各バイトＢに対し、

（ａ）１バイト以上のシリアルキーストリーム出力を発生し、

（ｂ）バイトＢをバイトＢおよびシリアルキーストリーム出力のうちの前記発生されたバイトに応じた値に置換することにより、暗号化されたビットストリームのうちのｉ番目の部分C_iを形成する工程とを備えた、シリアルキーストリーム出力と二進情報Ｐとを組み合わせる方法。

１２．連続する各部分P_iに対して、開始点からP_iまで（P_iを含む）の二進情報Ｐのすべての部分に対する累算的な現在メッセージダイジェスト値D_iを計算する工程と、現在のメッセージダイジェスト値D_iに依存する数の付加的バイトのシリアルキーストリーム出力を得てこれを廃棄する工程を更に含む、請求項１１記載の、シリアルキーストリームと二進情報とを組み合わせる方法。

１３．一連の部分P_iを含む二進情報Ｐを再現するよう、各部分C_iが多数のバイトn_iを含む一連の部分C_i、....、C_Nを含む暗号化されたビットストリームＣとシリアルキーストリーム出力とを組み合わせる方法であって、

各連続する部分C_iに対し、

（１）複数のバイトのシリアルキーストリーム出力を使用して数１、....、ｎの疑似ランダム順列Ｔを発生する工程と、

（２）部分C_iの各バイトＢに対して、

（ａ）１以上のバイトのシリアルキーストリーム出力を発生し、

（ｂ）バイトＢを、バイトＢおよびシリアルキーストリーム出力の前記発生されたバイトに応じた値で置換することにより、中間部分I_iを形成する工程と、

（３）前記二進情報のｉ番目の部分P_iを形成するよう、順列Ｔに従って中間部分I_i内のバイトの相対位置を順列する工程とを備えた、シリアルキーストリ

ーム出力と暗号化されたビットストリームとを組み合わせる方法。

１４．連続する各部分P_iに対して、開始点からP_iまで（P_iを含む）の二進情報Ｐのすべての部分に対する累算的な現在メッセージダイジェスト値D_iを計算する工程と、現在のメッセージダイジェスト値D_iに依存する数の付加的バイトのシリアルキーストリーム出力を得てこれを廃棄する工程を更に含む、請求項１４記載の、シリアルキーストリームと暗号化されたビットストリームとを組み合わせる方法。

１５．公開キー暗号システムで使用するのに適したミクスチャー発生器であって、

一組（ｎ）の最大期間線形シフトレジスタ発生器と、

前記ｎ個の発生器をクロック制御するための手段と、

混合されたキーストリームを発生するよう、前記発生器のｎ－１の出力を逐次選択するための手段と、

ｎ番目の発生器の複数の最後のｍ個のステージの出力をデコードするためのデコード手段とを備え、

該デコード手段の出力が、各クロック期間中に使用する特定の発生器の出力の選択の際に、前記選択手段を制御するミクスチャー発生器。

１６．ｎ＝３であり、ｍ＝１である、請求項１５記載のミクスチャー発生器。

【発明の詳細な説明】

非決定論的公開キー暗号化システム

技術分野

本発明は暗号システムに関し、特に計算上安全な公開キー暗号化システムおよびデジタルサイン（認証）システムを実現するための方法および手段に関するが、これらに限定されるものではない。

背景技術

最近の通信システムの設計において、データの安全性（セキュリティ）は次第に重要な事柄となっている。オブザーバー（すなわち侵入者）に対して通信中のメッセージが無意味に見えるよう、メッセージをスクランブルまたはコード化する試みとして、これまで暗号化システムが考案されている。暗号化システムの多くはキーのアイデアを利用しており、まず通信しようとするメッセージを発信者がこのキーでコード化し、メッセージの受信者がこのキーを用いてこれをデコードするようになっている。このタイプの従来の暗号化システムでは、メッセージの予定する受取人がメッセージを解読する前に、メッセージの発信者が予定する受信者にまず暗号解読キーを送らなければならないという欠点がある。更に暗号化キーを変えるにはこれに対応して暗号解読キーも変えなければならず、この暗号解読キーを予定する受信者に送信しなければならない。受信者へのキーの送信時にはオブザーバーすなわち侵入者がこのキーを見つけるという危険が常にある。

このように、キーを交換し合わなければならないという問題を克服するため、公開キー暗号化システムが開発された。このタイプのシステムは、１９７６年にジフィエおよびヘルマン両氏によって提案されたものであり、このシステムでは通信システムへの各加入者は２つのキー、すなわち通信システムのすべての加入者が公に利用できるようにされている公開キーと、各加入者自らが維持するプライベートキーを有する。各加入者のプライベートキーは（選択またはランダム選択）のいずれかにより決定され、プライベートキーから公開キーが発生されるようになっている。プライベートキーは符号化キー（Ｅ）と考えることができるが、

プライベートキーは暗号解読キー（Ｄ）と考えることができる。

公開キー暗号化システムはキーの間に存在する数学的関係が、一方向関数となっていることが多い。すなわち公開キーはプライベートキーより比較的容易に発生できるが、公開キーからプライベートキーを決定することは計算的に不可能である（すなわち計算的リソースの数が多数である場合に、プライベートキーの決定は恐らく一生かかってもできないことであろう）。

加入者Ａが公開キー暗号化システム内の加入者Ｂへメッセージｍを送信できるようにするため、ユーザーＡは、まず公開利用可能なレジスタすなわちファイルからユーザーＢの公開キーを得て、これを利用してメッセージｍを暗号化する。暗号文Ｃはメッセージｍを暗号化した結果であり、ユーザーＢへ送信され、ユーザーＢは自分のプライベートキーを用いて暗号文Ｃを変換し、メッセージｍを得る。

メッセージｍの発見を望み、公開キーを知っており、恐らく暗号システムに完全な知識をも有するオブザーバーすなわち侵入者にとって、公知のキーからプライベートキー（暗号解読キー）を決定しなければならない。先に述べたように、このシステムはこのような演算が極端に実行困難であるという事実に基づいている。他方、侵入者は何も得ることができず、侵入した暗号化メッセージとメッセージ言語の統計的性質の限られた知識しか有することができない。

リベスト外に付与された米国特許第4,405,829号には、公開キー暗号化システムの一例が開示されている。ここに開示されている一方向関数は極めて大きい数の因数分解は極めて困難であるという事実を活用するものである。しかしながらこのシステムは、大きな（例えば５１２ビットの）整数の広範な乗算が必要であり、これは極めて低速なプロセスとなるという欠点がある。このシステムの別の欠点としては、使用される暗号化方法は完全に決定論的であるということである。すなわち、同一の受信者に同一のメッセージを後で送信した場合、同一の暗号文が発生され、これにより侵入者すなわち盗聴者が送信中のメッセージトラフィックから重要な情報を得ることが可能となる。別の欠点としては、工学上の妥協、すなわち速度と安全性の妥協を図ることができず、一方、種々のタイプの暗号システム、例えば極端に高速で適度な安全性を備えた暗号システム、または適度

に

高速で安全性の高いシステムを設計できるという利点がある。更に別の欠点としては、汎用デジタルコンピュータと異なり極めて高速の特殊用電子デバイスを使って実現すると、このシステムは大きくなって扱いにくいことが挙げられる。

安全な通信システムの別の好ましい性質としては、メッセージの発信者として表示された加入者がメッセージの真の発信者であるということを最終的に証明できることが挙げられる。これがいわゆるサインおよび認証の問題である。

ヘルマン外に付与された米国特許第4,200,770号には、提案された公開キー発送システムの従来の例が開示されている。しかしながら、この提案されたシステムは真の公開キー暗号化システムというよりも、むしろキー交換システムである。ヘルマンおよびジフィエは、１９７９年３月のＩＥＥＥの議事録の第６７巻第３号、第４０１頁に公開された論文「プライバシーおよび認証：暗号化技術入門」において、デジタルサイン方式も提案している。ここに開示されたサインシステムでは、メッセージＭを加入者Ｂへ送りたいと望む加入者Ａは、まず自分のプライベートキーを用いてメッセージ文Ｍを暗号化し、この結果をユーザーＢの公開キーを用いて、この結果を暗号化し、ユーザーＢへ送信する暗号文Ｃを発生する。次にユーザーＢは、自分のプライベートキーを利用してユーザーＢの公開キーによる更なる変換によってメッセージ文Ｍが発生されるようなフォームへ暗号文を変換する。一連のステップ後、メッセージが再現される場合、メッセージはユーザーＡから来たものに違いないことが判る。

このシステムの１つの欠点は、発信者および受信者の双方が暗号化プロセスを２回実行しなければならず、プロセスの速度に悪影響が及ぶ。別の欠点としては、メッセージの暗号解読をするため発信者の公開キーを知る必要があり、このことは公開キーファイルへのアクセスの需要が大きくなることが挙げられる。更に別の欠点としては、古いキーを無効とした後でも古い公開キーを維持し、識別する必要があり得ることによって、公開キーファイルの管理の問題が複雑となることが挙げられる。更に別の欠点としては、プライバシーおよび認証の双方での役割を果たすのに公開キーファイルが必要であるということが挙げられるが、一方

、これら全く異なる機能を達成するのに必要な情報を別々に管理できるという利点もある。

発明の開示

従って、本発明の目的は上記欠点を克服するか、または少なくとも業界に有効な選択案を提供する、完全な公開キー暗号化システムを提供することにある。

従って１つの特徴によれば、本発明は、メッセージ発信者がメッセージ受信者に固有の公知のキーを使って平文メッセージＰを暗号化し、メッセージ受信者が公開キーを発生した秘密のプライベートキーを使用して暗号化メッセージを暗号解読する公開キー暗号システムにおいて、

（１）複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、

（２）前記数$D_{1\sim n}$の各々に対してプライベートキー$D_{1\sim n}$によって得られた対応する数に等しい数のクロックパルスまたはステート変化の後に所定の公知の初期ステートから疑似ランダム二進数発生器のステートを発生し、公開キー（Ｅ）の成分として計算された二進ステート$E_{1\sim n}$の各々を提供することによりプライベートキーを用いて（先に記載した）累乗により公開キー（Ｅ）を計算し、

（３）メッセージ発信者が、

（ａ）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を発生し、数$R_{1\sim n}$の各々に対してランダム初期化キー$R_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の公知の初期ステートから疑似ランダム二進数発生器のステートを計算し、オープンキーＱの成分として計算された二進数ステート$Q_{1\sim n}$を提供することにより、累乗によりオープンキーＱを計算し、

（ｂ）公開キーＥの成分をランダム初期化キーＲの成分により累乗し、前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対し、工程（２）に記載の方法を対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じた疑似ランダム二進数発生器のステートを計算することにより、発生器初期化ステート$K_{1\sim n}$を発生し、

（ｃ）第１ミクスチャー発生器を形成するように出力が組み合わされている一組（ｎ）の疑似ランダム二進数発生器に初期値$K_{1\sim n}$をロードし、

（ｄ）キーストリームシリアル出力を得るように、ミクスチャー発生器をクロックし、その出力と二進平文メッセージとを組み合わせ、暗号化されたビットストリームを発生し、

（ｅ）オープンキーＱと共に暗号化されたビットストリームをメッセージ受信者に送信し、

（４）メッセージ受信者が、

（ａ）メッセージストリームからオープンキーＱを抽出し、

（ｂ）ステップ（３）（ａ）に記載の方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することにより得られる疑似ランダム二進数発生器のステートを、前記数$Q_{1\sim n}$および$D_{1\sim n}$の各々に対して計算することにより、発生器初期化ステート$K_{1\sim n}$を発生するようにオープンキーＱをプライベートキーＤで累乗し、

（ｃ）ミクスチャー発生器を形成するように出力が組み合わされた第２の組（ｎ）の疑似ランダム二進数発生器に発生器初期化ステート$K_{1\sim n}$をロードし、

（ｄ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力と受信した暗号化ビットストリームとを組み合わせて発信者の平文メッセージを発生することを特徴とする、公開キー暗号システムから成る。

第２の特徴によれば、本発明は、複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、前記数$D_{1\sim n}$の各々に対しプライベートキー$D_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$E_{1\sim n}$の各々を公開キーＥの成分として提供することにより、プライベートキーを使用して公開キー（Ｅ）を累乗する、公開キー暗号システム用の暗号化装置であって、

一組の二進数$R_{1\sim n}$を備えたランダム初期化キー（Ｒ）を発生するための手段と、

前記数$R_{1\sim n}$の各々に対しランダム初期化キーR$_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変換の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$Q_{1\sim n}$の各々をオープンキーQの成分として提供することにより、各番号を使って初期値を累乗するための手段と、

前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対し、公開キーEを累乗するのに使用される

方法を対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するよう、公開キーEの成分をランダム初期化キーRの成分で累乗するための手段と、

ミクスチャー発生器の出力を形成するように出力が組み合わされた一組（ｎ）の疑似ランダム二進数発生器を含むミクスチャー発生器と、

前記組（ｎ）の疑似ランダム二進数発生器に$K_{1\sim n}$に等しい初期値をロードする手段と、

キーストリームシリアル出力を得るようにミクスチャー発生器をクロック化する手段と、

平文メッセージを受信し、ミクスチャー発生器の出力と二進平文メッセージとを組み合わせ、暗号化されたビットストリームを発生する手段と、

オープンキーQと共に暗号化されたビットストリームをメッセージ受信者に送信するための手段とを備えた、公開キー暗号システムのための暗号化装置から成る。

第３の特徴によれば、本発明は、複数の二進数$D_{1\sim n}$を含むプライベートキー（Ｄ）を選択し、前記数$D_{1\sim n}$の各々に対しプライベートキー$D_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算した二進ステート$E_{1\sim n}$の各々を公開キー（Ｅ）の成分として提供することにより、プライベートキーを使用して公開キー（Ｅ）を累乗し、

メッセージ発信者が、

（１）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を選択し、前記数$R_{1\sim n}$の各々に対しランダム初期化キー$R_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の公知の初期ステートから疑似ランダム二進数発生器のステートを計算し、オープンキーＱの成分として計算された二進数ステート$Q_{1\sim n}$を提供することにより、各数を使って初期化ステートを累乗し、

（２）公開キーＥの成分をランダム初期化キーＲの成分により累乗し、プライベートキーを用いて公開キーを累乗すると先に定義した方法を、対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似ランダム二進数発生器のステートを前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対して計算することにより、発生器初期化ステート$K_{1\sim n}$を発生し、

（３）第１ミクスチャー発生器を形成するように出力が組み合わされている疑似ランダム二進数発生器の組（ｎ）に初期値$K_{1\sim n}$をロードし、

（４）キーストリームシリアル出力を得るように、第１ミクスチャー発生器をクロックし、この出力と二進平文メッセージとを組み合わせて暗号化されたビットストリーム暗号文Ｃを発生し、

（５）オープンキーＱとともに、暗号化されたビットストリームをメッセージ受信者に送信するような方法に従って平文メッセージを暗号化し、

暗号解読装置が、

暗号化されたビットストリームからオープンキーＱを抽出するための手段と、

前記数$Q_{1\sim n}$および$D_{1\sim n}$の各々に対し、オープンキー（Ｑ）を発生するよう上記記載の方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することにより生じた疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するようプライベートキーＤの成分によりオープンキーＱの成分を累乗するための手段と、

ミクスチャー発生器を形成するよう出力が組み合わされた一組（ｎ）の疑似ランダム二進数発生器と、

前記組（ｎ）の疑似ランダム二進数発生器に$K_{1\sim n}$に等しい初期値をロードする手段と、

キーストリームシリアル出力を得るよう、ミクスチャー発生器をクロック制御するための手段と、

この出力と受信された暗号文とを組み合わせて平文メッセージを発生するための手段とを備えた、公開キー暗号システムのための暗号解読装置から成る。

第４の特徴によれば、本発明は、メッセージ発信者がメッセージにサイン情報を添え、公衆が検査できるようにオープンにされたサインアーカイブに発信者の名前と共に対応する認証情報を登録し、メッセージ証明者がメッセージおよびそのサイン情報、更に公共サインアーカイブからの認証情報を得て、これらを使って前記サイン情報によって識別された発信者によりメッセージが送られたものであるかどうかを確認する、公開キー認証システムにおいて、

（１）メッセージ発信者が、

（ａ）複数の二進数$S_{1\sim n}$から成るランダムデジタルサイン（Ｓ）を選択し、

（ｂ）前記数$S_{1\sim n}$の各々に対しランダムデジタルサイン$S_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定の初期ステートから疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$V_{1\sim n}$の各々を証明キーＶの成分として提供することにより、証明キーＶを累乗し、

（ｃ）工程（ｂ）において計算された証明キーＶがまだ登録されたものでないかどうか確認するよう前記サインアーカイブをチェックし、先に登録されたものであれば工程（ａ）、（ｂ）を繰り返し、

（ｄ）一組（ｎ）の疑似ランダム二進数発生器のうちの各々に対して、送信されたメッセージを含むビットシーケンスを前記ランダム二進数発生器に対応する法で割ることによって得られる剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チック（ＣＲＣ）値Ｃの成分として提供することにより、ＣＲＣ値Ｃを計算し、

（ｅ）合計Ｃ＋Ｓ（モジュロ２）を計算し、公共サインアーカイブ内にメッセージ送信者の名前でこの合計および証明キーＶを登録し、

（ｆ）Ｓを送信メッセージに添え、

（２）メッセージ証明者が、

（ａ）メッセージから複数の二進数$S_{1\sim n}$を備えたデジタルサイン（Ｓ）を抽出し、

（ｂ）前記数$S_{1\sim n}$の各々に対して、受信したメッセージを含むビットシーケンスを疑似ランダム二進数発生器に対応する法で割ることによって得られる剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チェック（ＣＲＣ）値Ｃの成分として提供することにより、ＣＲＣ値Ｃを計算し、

（ｃ）前記数$S_{1\sim n}$の各々に対し工程（１）（ｂ）に記載された方法により前記各数$S_{1\sim n}$を使用して対応する疑似ランダム二進数発生器の所定初期値を累乗することにより証明キーＶを計算し、

（ｄ）合計Ｃ＋Ｓ（モジュロ２）を計算し、

（ｅ）値Ｃ＋Ｓ（モジュロ２）と工程（ｃ）および（ｄ）で計算されたＶが一致する認証情報を探すよう、メッセージのうちの前記サイン情報によって識別される発信者の名前で公共サインアーカイブをサーチし、

（ｆ）工程（Ｅ）におけるサーチが成功した場合、メッセージを正しいものと認め、または工程（ｅ）におけるサーチが成功しなかった場合、メッセージを偽物として拒否することを特徴とする、公開キー認証システムから成る。

第５の特徴によれば、本発明は、メッセージ認証者が複数の二進数$D_{1\sim n}$を含むプライベートキーＤを選択し、前記数$D_{1\sim n}$の各々に対しプライベートキー$D_{1\sim n}$によって示された対応する数に等しい数のクロックパルスまたはステート変化の後に、所定初期ステートから疑似ランダム二進数発生器のステートを計算し、計算した二進ステート$E_{1\sim n}$の各々を公開キーＥの成分として提供することにより、プライベートキーを用いて公開キーＥを累乗し、公開キーを公衆の検査ができるようにし、メッセージ発信人が前記メッセージ認証者と共に固有の認証情報を登録し、メッセージにサイン情報を添え、メッセージ証明者がメッセージを

得て、メッセージのための一般化されたＣＲＣ値を計算し、メッセージサイン情報、一般化されたＣＲＣ値および発信者の名前またはその他の識別情報をメッセージ認定者へ送り、前記メッセージ認証者が前記一般化されたＣＲＣ値、前記メッセージサイン情報および前記登録された認証情報を使用して、メッセージが前記認証情報によって識別された発信者によって送信されたものであるかどうかを確認する、公開キー認証システムにおいて、

（１）メッセージ発信者が、

（ａ）複数の二進数から成る認証パスワード（Ｐ）を選択し、

（ｂ）認証パスワードＰを登録し、発信者の名前または他の識別情報に対応させ、Ｐが他人によって登録されていないかどうかを確認することを前記サイン認証者に求め、Ｐがすでに登録されていると通知を受けた場合、工程（ａ）を

繰り返し、

（ｃ）一組（ｎ）の疑似ランダム二進数発生器の各１つに対し、送信メッセージを含むビットシーケンスを前記疑似ランダム二進数発生器に対応する法で割ることにより得られた剰余を計算し、かかる各剰余$C_{1\sim n}$を一般化された周期的冗長性チェック（ＣＲＣ）値C_Mとして提供することにより、一般化されたＣＲＣ値C_Mを計算し、

（ｄ）一般化されたＣＲＣ値C_Mを認証パスワードＰに添えることにより中間サイン情報を計算し、

（ｅ）（ｉ）一組の二進数$R_{1\sim n}$を含むランダム初期化キー（Ｒ）を選択し、前記数$R_{1\sim n}$の各々に対し、ランダム初期化キー$R_{1\sim n}$によって示される数のクロックパルスまたはステート変化の後に所定の初期値から疑似ランダム二進数発生器のステートを計算し、計算された二進ステート$Q_{1\sim n}$の各々を提供して、オープンキーＱを発生することにより各数を用いて初期値を累乗し、

（ｉｉ）前記数$E_{1\sim n}$および$R_{1\sim n}$の各々に対しプライベートキーを用いて公開キーを累乗すると先に記載した方法を、対応する二進数$R_{1\sim n}$に等しい回数だけ適用することによって生じる疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するよう、サイン

認証公開キーＥの成分をランダム初期化キーＲの成分で累乗し、

（ｉｉｉ）ミクスチャー発生器を形成するように出力が組み合わされた一組（ｎ）の疑似ランダム二進数発生器に初期値$K_{1\sim n}$をロードし、

（ｉｖ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力と前記中間サイン情報とを組み合わせ、暗号化された中間サイン情報を発生し、

（ｖ）該暗号化された中間サイン情報を前記オープンキーＱに添えてメッセージサイン情報$S_{P,M}$を発生することによってサイン認証公開キーＥを使って工程（ｄ）で計算された中間サイン情報を暗号化することによりメッセージサイン情報$S_{P,M}$を計算し、

（ｆ）該メッセージサイン情報$S_{P,M}$をメッセージに添え、更に発信者の名前またはその他の識別情報をメッセージに添え、

（２）メッセージ証明者が、

（ａ）メッセージからメッセージサイン情報（$S_{P,M}$）および発信者の名前または他の識別情報を抽出し、

（ｂ）工程（１）（ｃ）に記載された方法によりメッセージに対する一般化されたＣＲＣ値C'_Mを計算し、

（ｃ）該メッセージサイン情報、発信者の名前、または他の識別情報および前記一般化されたＣＲＣ値C'_Mをサイン認証者へ送り、該サイン認証者にメッセージサイン情報$S_{P,M}$内の暗号化された認証パスワードＰおよび一般化されたＣＲＣ値C_Mと、C'_Mおよび発信者の名前または他の識別情報とを比較することを求め、

（３）メッセージ認証者が、

（ａ）（ｉ）メッセージサイン情報からオープンキーＱを抽出し、

（ｉｉ）前記数$Q_{1\sim n}$および$D_{1\sim n}$の各々に対し工程（１）（ｅ）（ｉ）に記載された方法を対応する二進数$D_{1\sim n}$に等しい回数だけ適用することによって得られる疑似ランダム二進数発生器のステートを計算することにより、発生器の初期化ステート$K_{1\sim n}$を発生するよう、オープンキーＱをプライベート

キーDで累乗し、

（ｉｉｉ）ミクスチャー発生器を形成するように出力が組み合わされた第２の組（ｎ）の疑似ランダム二進数発生器に発生器の初期化ステートK_1～nをロードし、

（ｉｖ）キーストリームシリアル出力を得るようにミクスチャー発生器をクロック制御し、この出力とメッセージサイン情報とを組み合わせて工程（１）（ｄ）で計算された中間サイン情報ＰおよびＣを再現することにより、プライベートキーＤを用いてメッセージサイン情報$S_{P,M}$を暗号解読し、

（ｂ）前記中間サイン情報に含まれたＰの値と、工程（２）（ｃ）で送られた名前または他の識別情報に対応して登録された認証パスワードとを比較し、

（ｃ）前記中間サイン情報に含まれたC_Mの値と、工程（２）（ｃ）で送られたC'_Mの値とを比較し、

（ｄ）工程（ｃ）および（ｄ）における双方の比較に成功した場合、メッセージが正しいものであることをメッセージ証明者に確認し、いずれかの比較に失敗した場合、偽物としてメッセージを拒否することを特徴とする、公開キー認証システムから成る。

第６の特徴によれば、本発明は、

（１）ユーザーがある時間ｔにおけるステートが複数の座標（X_{t1}、X_{t2}、.....、X_{tn}）によって示された点X_1として表示できる電子ポインタデバイスを操作する工程と、

（２）複数の時間ｔ＝１、２、....、ｎにおける前記入力デバイスのステートを表示する点X_1を測定する工程と、

（３）前記時間のサブセットに対応する、上記のように測定された点のサブセットを選択する工程と、

（４）このように選択された点すべての座標の数値関数を計算する工程と、

（５）このように計算された数値関数の値を示す複数の二進数として、所望の乱数を得る工程とを備えた、乱数を発生するための方法から成る。

第７の特徴によれば、本発明は、一連の部分C_iを含む暗号化されたビットス

トリームＣを発生するよう、各部分Ｐ$_i$が多数のバイトｎ$_i$を示す一連の部分Ｐ１、．．．、Ｐ$_N$を備えた二進情報Ｐとシリアルキーストリーム出力とを組み合わせる方法であって、

（１）シリアルキーストリーム出力の複数のバイトを使用してバイト１、．．．、ｎ$_i$の疑似ランダム順列Ｔを発生する工程と、

（２）中間部分Ｉ$_i$を形成するよう、順列Ｔに従って部分Ｐ$_i$内のバイトｎ$_i$の相対位置を順列する工程と、

（３）中間部分Ｉ$_i$の各バイトＢに対し、

（ａ）１バイト以上のシリアルキーストリーム出力を発生し、

（ｂ）バイトＢをバイトＢおよびシリアルキーストリーム出力のうちの前記発生されたバイトに応じた値に置換することにより、暗号化されたビットストリームのうちのｉ番目の部分Ｃ$_i$を形成する工程とを備えた、シリアルキーストリーム出力と二進情報Ｐとを組み合わせる方法から成る。

第８の特徴によれば、本発明は、一連の部分Ｐ$_i$を含む二進情報Ｐを再現するよう、各部分Ｃ$_i$が多数のバイトｎ$_i$を含む一連の部分Ｃ$_1$、．．．．、Ｃ$_N$を含む暗号化されたビットストリームＣとシリアルキーストリーム出力とを組み合わせる方法であって、

各連続する部分Ｃ$_i$に対し、

（１）複数のバイトのシリアルキーストリーム出力を使用して数１、．．．．、ｎ$_i$の疑似ランダム順列Ｔを発生する工程と、

（２）部分Ｃ$_i$の各バイトＢに対して、

（ａ）１以上のバイトのシリアルキーストリーム出力を発生し、

（ｂ）バイトＢを、バイトＢおよびシリアルキーストリーム出力の前記発生されたバイトに応じた値で置換することにより、中間部分Ｉ$_i$を形成する工程と、

（３）前記二進情報のｉ番目の部分Ｐ$_i$を形成するよう、順列Ｔに従って中間部分Ｉ$_i$内のバイトの相対位置を順列する工程とを備えた、シリアルキーストリーム出力と暗号化されたビットストリームとを組み合わせる方法から成る。

図面の簡単な説明

第１図は、本発明を実施するのに利用できるＭＬＳＲＧ成分発生器を備えたミクスチャー発生器の図である。

第２図は、第１図のミクスチャー発生器、すなわちジェフ（Geffe）タイプの発生器の好ましい実現例の図である。

第３図は、第２図に示されたシフトレジスタの構成例の図である。

第４図は、暗号化装置のハードウェアの実現例のブロック図である。

第５図は、暗号解読器のハードウェアの実現例のブロック図である。

発明を実施するための最良の態様

次の説明は、本発明の好ましい実施例を開示するものであり、そのいくつかの変形例も述べている。本文献における記載は、デジタルコンピュータにおいてソフトウェアで本発明を実現するという観点からのものであるが、特殊用の電子ハードウェア構成部品を用いて全システムのすべてまたは一部を実現することも可能であると理解すべきである。かかる成分構成部品としては論理素子、例えばＬＳＩメモリ、シフトレジスタ、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）およびディスクリートロジックがあるが、これらのみに限定されるものではない。

１．本発明の分類

時々、非対称キーシステムと称される公開キー暗号システムの分類方法は、プライベートキー／公開キーのペアに関連する一方向関数のタイプに従うものであり、特に一方向関数を反転するため、（すなわち公開キーからプライベートキーを推定するため）解くことが必要な数学的問題に従っている。かかる３つの問題は、これまで提案された実質的にすべての公開キーシステムから生じるものである。すなわち素因数分解、離散的対数およびナップサック（knapsacks）の問題が生じている。例えば、最も知られている公開キーアルゴリズム、すなわちＲＳＡは、大きな整数の素因数分解が困難なことに基づく方法である。真の公開キー暗号システムというよりもむしろ、公開キー配送システムであるジフィエーヘルマン方法は、エルガマル（Ｅｌ　Ｇａｍａｌ）公開キー暗号システムのような離

散的対数問題に基づくものである。

本システムは数学的な用語では、離散的対数問題に基づくものである。このことは、本システムでは有限体における累乗法に数学的に等価的な演算を用いてプライベートキーから公開キーを計算することを意味する。従って、公開キーからプライベートキーを計算する意図でこのシステムを破壊するには、侵入者は有限体に対する対数を計算しなければならない。計算上の効率、簡潔性およびスピードのみならず、安全性の理由から、本システムの機素となる有限体はガロア体ＧＦ［2^p］であり、更にｐは2^p-1が大きな素数（メルセンヌ素数）となるように選択したものである。後に理解できるように、このシステムは２つ以上のかかる体に対する累乗を実施するものである。

暗号化システムを分類する別の方法は、決定論的であるかまたは非決定論的であるかどうかに関連する。非決定論的暗号システムに最初に言及したものは、カールニコライによると考えられる。名称は多数の方法で多少正確に記載できるが、非決定論的暗号システムの性質の１つは、同じキーを２回以上、所定の平文を暗号化するのに用いた場合でも、これから得られる暗号文は非システマティックに、理想的には真にランダムに異なるというのが、非決定論的暗号システムの特徴の

１つである。本システムは非決定論的暗号システムである。

平文を暗号文に変換する際、暗号システムは元の平文の長さを増減したり、またはそのままにしておくことができる。本システムは暗号文に短いヘッダーブロックを添えることを除き、平文と全く同じ長さの暗号文を発生する。このヘッダーブロックの長さは特定の実現例に体して選択されたパラメータに応じて決まるが、一般に６４～２５６バイトの長さとなる。そのフォーマットは重要ではない。

２．ミクスチャー発生器

本発明の中心となる構成要素は、独立した同一分布ランダム変数のミクスチャー（混合数）の確率理論から得られる概念との類似により、ここでミクスチャー発生器と称する新しいタイプの疑似ランダム二進キーストリーム発生器である。

混合数発生器は単一の疑似ランダム二進数発生器、例えば最大期間リニアシフトレジスタ発生器（ＭＬＳＲＧ）または最大期間乗算的合同発生器（ＭＣＧ）から成り、これら発生器の出力すなわちステートは他の成分疑似ランダム二進数発生器の組のうちの１つの構成要素（項）をメモリレス状に連続的に選択するのに使用される。第１図はミクスチャー発生器を示し、ここではミキサー発生器G_mは最大期間リニアシフトレジスタとなっており、このレジスタの時間Ｔにおける最後の３つのステージは時間Ｔにおいて出力を使用すべき他の８つのＭＬＳＲＧ（G_0、....、G_j、....、G_7）の１つを選択するのに使用される。ミキサー発生器G_mのクロックレートは成分発生器G_jのクロックレートの３倍とみなすことができる。図２に示されるより簡単な例は、この特殊なケースであり、ジェフ発生器として知られるものである。第２図において、ミキサー発生器G_mの最後のステージは時間Ｔにおけるミキサー出力が１である場合には、頂部の発生器G_tの出力を選択し、Ｔにおけるミキサー出力が０である場合には、底部の発生器G_bの出力を選択する。より詳細には、このような構成の具体例としては、ミキサー発生器が（原始）生成三項式$1+x^{38}+x^{89}$を備えた８９のステージを有し、頂部の発生器が（原始）生成三項式$1+x^{30}+x^{127}$を備えた１２７のステージを有し、底部の発生器が（原始）生成三項式$1+x^{168}+x^{521}$を備えた５２１のステージを有するような場合である。より小さい（および安全性の低い）場合は３つの発生器がそれぞれの三項式$1+x^{13}+x^{87}$、$1+x^{38}+x^{89}$および

$1+x^{30}+x^{127}$に対応する例である。成分発生器としてＭＬＳＲＧを使用する場合、生成多項式が原始多項式となるような発生器を使用することが重要である。更に、かかる発生器は素数の数のステージを有し、それらの時間長さがメルセンヌ素数となるような性質を有することができる。

本明細書の残りの部分では、記号ｐ（ｘ）をＭＬＳＲＧに対応する生成多項式を表示するのに使用する。

本明細書で定義するミクスチャー発生器は必ずしもＭＬＳＲＧまたはＭＣＧ成分から成る成分発生器に限定する必要はない。むしろ、ミキサーを含む構成部品はミクスチャー発生器自体でもよいし、または好ましい統計的、すなわち暗号特

性を備えた他のタイプの非線形発生器でもよい。

ミクスチャー発生器はディスクリート論理回路またはカスタム集積回路のいずれかを使用する極めて高速の特殊用ハードウェアで実現するか、または汎用コンピュータでソフトウェアによりシミュレートすることができる。

ミキサー発生器は、ミキサーおよび他の成分発生器の特殊ステートから開始する有限ステートデバイスであるので、このミキサー発生器は周期的二進シーケンス（すなわち永続的に繰り返される０と１のシーケンス）を発生するのに使用できる。発生器のステートはその成分の各々の各ステージのステートを特定する二進値の組により記述される。

ミキサー発生器の構造の利点としては、それらの期間が極めて長く、極めて複雑であり、０と１の分布のバランスが良好にとれており、連続する出力に実質的に相関性がないということが挙げられる。これらの出力はＮ個の要素の分散および実行上の統計の点で優れた統計的性質を有する。数学的に実証できるこれら性質もあれば、（例えばχ二乗分布または実行テストを使用することにより）既に実証されている性質もある。

周期的二進シーケンスはある種のＭＬＳＲＧによって発生でき、暗号用のシーケンスの適性を評価する際の臨界ファクターの１つは、このシーケンスを発生するのに必要な最短線形フィードバックシフトレジスタの長さにある。ミクスチャー発生器の構成の大きな利点としては、ミキサーおよび成分発生器の長さに応じてその長さを正しく特徴づけることが容易となることが多いこと、および発生器の複雑さの良好な目安となる長さ、従って暗号用の有効性が極めて高いということが挙げられる。

次に、図２に示されたジェフタイプのミクスチャー発生器を参照して本発明の暗号システムにおけるミクスチャー発生器の使用法について説明する。まず、ミキサー、頂部発生器および底部発生器を形成するＭＬＳＲＧにおけるステージの数をn_m、n_tおよびn_bとそれぞれ表示し、それぞれの発生器の初期ステート（時間Ｔ＝０における）をそれぞれa_{m0}、a_{t0}およびa_{b0}と表示する。ここで、便宜上これら初期ステートの各々は固定されており、公知であるとする。本発明の

変形例としてはユーザーの特定グループのメンバー間で安全かつ認証されたメッセージ送信を可能にするように、この特定グループだけにしか知られていないキーの一部として初期ステートを使用することが考えられる。

n_m＝８７、n_t＝８９およびn_b＝１２７を備えたこのタイプのミクスチャー発生器を使用するパソコンでのファイル暗号化により適性な安全レベルを備えた極端に高速のシステムが得られる。n_m＝８９、n_t＝１２７およびn_b＝５２１と選択することにより、パソコンでもより安全性の高いシステムが得られる。後者の３つの数はいずれもメルセンヌ素数を生じるものである。

ジェフタイプの発生器の時間（すなわち発生器の出力が繰り返した後のクロックサイクル数）は、成分発生器の時間の積、すなわち（$2^{n_m}-1$）（$2^{n_t}-1$）（$2^{n_b}-1$）となることを数学的に証明できる。同じ出力シーケンスを発生できる最も短い等価的線形シフトレジスタにおけるステージ数で示される発生器の複雑度は、$n_m n_t + (1+n_m) n_b$で計算できる。類似の結果により、より複雑なミクスチャー発生器を分析することもできる。

３．一方向関数を実現するためのミクスチャー発生器の使用

ミクスチャー発生器によって発生される極めて長い二進シーケンスは多くの有効な性質を有する。出力ストリームおよびその内部ステートのシーケンスを得るのに、実際に発生器を作動させる、すなわちクロック制御することが可能である。発生器の時間はかなり長いので、どれだけ速く発生器をクロック制御しても、妥当な時間内にすべての出力ストリームのうちの一部のセグメントしか発生できない。上記例の発生器より小さい発生器でも、時間長さは2^{303}の大きさとなる。

ミクスチャー発生器を使用すれば公知の開始ステートから開始して特定の回数（どれだけの多くの回数でも）だけ、個々の成分をクロック制御した場合の最終内部ステートがどのステートになるかを高速かつ効率的に計算することが可能である。

しかしながら、逆の問いに対して計算で答えることはできない。すなわち、各成分に対し最終ステートが判っていても公知の開始ステートから初めてかかる最

終ステートに達するのに、各成分に対しどれだけの回数クロック制御することが必要であるかを決定するのは極めて困難である。この問いへの解答は、いわゆる離散的対数問題の解答方法にほとんど等しい。かかる問題を解くための公知の最良のアルゴリズムはＤ・コッパースミスによる方法であり、この方法は極めて効率的である。想像可能なコンピュータでこのアルゴリズムを実行するのに要する時間は極めて正確に予想できる。最も長い成分発生器が長さ１２７である場合、極めて高速のコンピュータで最も適度な時間長さで必要な計算を実施することが実際的であるが、最も長い成分発生器長さが５００以上の場合には当てはまらない。利用可能な計算能力に関する最も最適な予想のもとでも、かかる問題を解くことは計算的に不可能なままになっている。更に、発生器の長さを適当に選択することによる解答を得るうえの困難さを正確に処理できる。５００よりもかなり長い長さを備えた成分を含むミクスチャー発生器は実現するのに効率的であり、実際的である。

４．プライベートキーおよび公開キー

本システムではプライベートキーはミキサー発生器の成分をクロック制御すると仮定される任意の回数を指定する（二進）数の組に等価的である。これらの数は、各成分の周期的出力ストリーム内での（クロック数を単位として測定される）距離として解釈できる。

プライベートキーに対応する公開キーは、プライベートキーの対応する部分によって示される回数だけ各成分をクロック制御すべき場合に生じるミクスチャー発生器の最終ステートである。

このシステムにおいて使用されるプライベートキーと公開キーのペアと、他のほとんどのシステムで使用されるプライベートキーと公開キーのペアとの間には大きな違いがある。他の多くのシステムでは、特定の条件と制限に従ってキーのペアを同時に自動的に発生しなければならない。ＲＰＫシステムではプライベートキーの選択は完全に自由で制限されていない。このプライベートキーは、所望すれば指定されるよりもユーザーによって任意に選択できる。このことは、大きな実用的な利点であるばかりでなく、ＲＰＫシステムと他の特許された技術との

間の主要な違いも構成する。

図示されているジェフ発生器と関連させてプライベートキーの選択のためにユーザーＡは３つの数D_m、D_t、D_b（ここでD_mは１～$2^{n_m}-1$の範囲内にあり、D_tは１～$2^{n_t}-1$の範囲内にあり、D_bは１～$2^{n_b}-1$の範囲内にある）を選択するものとする。ここで、これら範囲の各各は上記限界値を含むが、厳密には範囲の大きい端部（二進ですべて１の値）は周期に等しいので、排除しなければならないことに留意されたい。ユーザーＡに対する公開キーは、D_m、D_tおよびD_bクロックサイクル（シフト）の後にそれぞれ３つの成分発生器のステートE_m、E_t、E_bを含む。ミクスチャー発生器、すなわちＮ個の成分発生器に対してプライベートキーおよび公開キーは３個でなくＮ個の成分ステートを有する。

プライベートキーまたは公開キーを形成するのに必要なビット数は$n_m+n_t+n_b$となり、この値は１つの例に対して使用される、より小さいほうのジェフ構造の場合には３０３であり、大きいほうの例に対する構造の場合では７３７であることに留意されたい。これらのビット数と広く使用されているＤＥＳの従来の暗号化アルゴリズムで使用される５６キービットとを比較することができる。

本発明の理解を完全にし、かつその理解を助けるため、所定のプライベートキーから公開キーを計算するための効率的な方法について次のとおり説明するが、このような説明は当業者には明らかであろう。これら方法の基礎となる数学上の理由から、所定のプライベートキーから公開キーを決定する方法を累乗法と称することが適当である。

ミクスチャー発生器の将来のステートを計算するための方法が必要であることは明らかである。この理由は、かかる発生器の時間が極めて長いことを考慮すれば、必要なステート数の一部より多くを発生するのに充分長くこれら発生器を実際に作動させることは不可能であるからである。線形フィードバックシフト（ＭＬＳＲＧ）レジスタ発生器の将来のステートを計算するための極めてコンパクトで効率的な方法が存在しており、この方法は、レジスタのステージの内容（すなわちそのステート）を１つの中間的ｘ内の多項式の係数として解釈することに基

づいている。レジスタはｎ個のステージを有するので、ステージの内容はｘの級数の係数、すなわち１，ｘ，x^2，....x^{n-1}を表すことができる。かかる多項式は次数がｎである先に述べた生成多項式ｐ（ｘ）と異なることに留意されたい。発生器のステージに０からｎ－１までの番号をつけ直すと便利である。ここで、ステージ０は中間発生器のタップの直後のステージに対応するので、ステージ（ｎ－１）は発生器の中間にあるフィードバックタップを備えたステージを示す。次に発生器の最終（出力）ステージには（ｎ－ｍ－１）の番号が付けられ、先と同じようにｍは生成多項式ｐ（ｘ）の中間項の指数を示す。

このような解釈を用いることにより、発生器のクロック制御から得られるステートが単一項ｘから成る多項式とそのステートを表示する多項式とを乗算した値に等しいことを証明できる。このような証明は、まずモジュロ２（すなわち１＋１＝０等）で係数に対するすべての演算を実行し、次に次数がｎ以上である場合の多項式の積が生成多項式ｐ（ｘ）の積モジュロを意味すると理解することにより行うべきである。この最後の説明はｎ以上の次数の多項式は、この多項式をｐ（ｘ）で除算した後の結果となるような残りと置換すべきであることを意味している。多項式の加算、乗算および除算は、通常の代数の規則に従うが、この場合における係数に対する演算をモジュロ２（ＸＯＲに等価的）で行うことは例外とする。

多項式をモジュロｐ（ｘ）で乗算するこのようなアイデアを１つのステップと考え、発生器の初期ステートa_0を０番号のついたステージにおける単一の１を備えたステートであるとみなせば、発生器を時間Ｄだけ進める（すなわち発生器をＤ回クロック制御する）方法は、積１・ｘ・ｘ・ｘ・....・ｘを計算することに等しい。ここで、因数ｘはＤ回を示す。この結果得られる積は、x^D モジュロｐ（ｘ）と表示できる。このようにＤを指数として使用することはx^D モジュロｐ（ｘ）を計算する効率的な方法では二進級数１，ｘ，x^2，x^4，x^8，……、x^{2k}、……、x^{2n-1}（すべてモジュロｐ（ｘ）である）を示す（ｎ－１）個の多項式をあらかじめ計算し、作表し、次にＤの二進表示内の１のビットに対応

する多項式を共に乗算（再び各時間ごとにモジュロｐ（ｘ）を行う）することが行われる。

多項式をモジュロｐ（ｘ）で乗算するこのような概念的方法は、実際にはシフトレジスタ自体を使って極めて簡単かつ効率的に実行できる。実際にはめんどうな乗算は不要である。

これを説明するため、発生器を１回クロック制御することは、その内容に対応する多項式をｘで乗算することに等しいので、すなわち発生器をｊ回クロック制御することにより$x^{\perp}$だけ乗算することができると考える。かかる中間的倍数に対応するステートを（例えばレジスタに）セーブし、対応する係数モジュロ２（すなわちＸＯＲ演算）するだけで任意の多項式の乗算を行う。このような方法により、モジュロｐ（ｘ）の積を小さくする際の多項式の除算をする別個の方法が不要となる。すべての方法を極めて短時間で行うための特殊な回路またはチップを設計することは、簡単なことであり、所望する場合にはソフトウェアで容易にエミュレートできる。

５．暗号化

上記のようにユーザーＡのためのプライベートキーＤは３つの番号（D_m、D_t、D_b）から成るが、ユーザーＡの公開キーＥは３つの番号（E_m、E_t、E_b）から成り、これら番号は公知であり、おそらく公共の住所録ファイルに記載されており、時間０における所定の公知の初期ステートa_0＝（a_{m0}、a_{t0}、a_{b0}）からスタートした時間D_m、D_tおよびD_bにおける対応する発生器のステーとを示す。多項式の表示における包括的なＭＬＳＲＧに対する時間およびステートを表示するのにＤおよびＥを等価的に使用することにより、初期ステートが０次の多項式１に対応すると仮定した$E-x^{D} \bmod p(x)$を有する。

暗号化すべき平文メッセージＰは、まずデータ圧縮することが好ましい。このデータ圧縮は、周知の技術であり、データ送信コストおよび／または記憶スペースを低減するのに有効であるのみならず、基礎となるメッセージの冗長性も低下する。これにより、暗号解読に失敗する可能性が増し、更に送信の誤りまたは暗号文の故意の変更（だまし）のいずれかから生じる誤りの伝搬も増やす。

（Ａのプライベートキーを使用する）ユーザーＡにしか解読できないよう、平文メッセージＰを暗号化するため、別のユーザーＢは、まずＰの暗号化中に限り使用すべきランダム初期化キーＲ＝（R_m、R_t、R_b）を発生する。Ｒは成分発生器に対する指数を表示するという点でＤに類似しており、Ｒの３つの成分はＤと同じ範囲内になければならない。ユーザーＢはプライベートキーＤから公開キーＥを計算するのと同じように、ＲからＱ＝（Q_m、Q_t、Q_b）を計算する。すなわちＱは初期ステートa_0からスタートし、時間Ｒにおける成分発生器のステートを示す。

ユーザーＢは次に、送信すべき、すなわちクリアに記憶すべき（すなわち暗号化すべき）暗号文のメッセージヘッダー内のＱを含める。このＱには通信用に有効な他の情報も含むことができる。例えば、特定のアプリケーションではメッセージヘッダー内にアドレス指定情報、周期的冗長性チェック（ＣＲＣ）バイトまたは他の誤り訂正データを含むことができる。

実際の暗号化方法を続けるには、ユーザーＢは次に成分発生器にＥ（ユーザーＡの公開キー）から成る初期ステートをロードし、次に、Ｒを指数とみなすＡの公開キーＡを累乗することにより、同じランダム初期化キーＲ＝（R_m、R_t、R_b）を使って最終ステートＫ＝（K_m、K_t、K_b）を計算する。多項式表示ではこれを$K_j = E_j^{R_j} \bmod p(x)$と記載することができる。ここでｊ＝ｎ、ｔ、ｂである。ユーザーＢはプライベートキーから公開キーを計算したのと同じようにミクスチャー発生器の成分シフトレジスタを使用しＡの公開キーの乗算により二進の級数E^{2k}（ｋ＝０、１、．．．．、ｎ－１）の積を計算する。

ここで、ユーザーＢはＫを計算するにあたりランダム初期化キーＲおよびユーザーＡの公開キーＥの双方を使用するだけでなく、初期ステートa_0の公に利用可能な知識および基礎となるミクスチャー発生器の構造も使用することに留意されたい。総合的な計算は、成分発生器のステートを２回（すなわちＱの計算に１回、更にＫの計算に１回）進めるのに必要な単なる多項式を累乗することとなる。ユーザーＢはＤを知ることなくＫを計算できたという事実にかかわらず、現在の暗号化システムの目的のためのＫの本質的な性質は、Ｋが発生器をまずＤだけ進

め、次にこの結果をＲで累乗することによって得られるステート（すなわちＲに等しい時間をＤで乗算した値だけ発生器を進めた場合の結果となる）を示すということである。

ステートＫは暗号文を発生し始める際に使用される最終発生器初期ステートとして使用される。ユーザーＢはステートＫから開始したミクスチャー発生器をクロック制御（作動）することによって得られたキーストリームを使用し、これを演算し、これと平文ビットストリームＰとを組み合わせることにより暗号文Ｃの本文を発生する。このような組み合わせ方法は、反転可能でなければならず（すなわちＫおよびＣが示された場合、平文Ｐを再現できなければならず）、種々の方法で実行できる。最も簡単な想像できる組み合わせ方法は、平文とキーストリームとをビットごとに単にＸＯＲ（排他的ＯＲ）演算することであるが、この方法は、使用した場合、深刻な暗号の欠陥を有する。

単純な組み合わせ方法は多数可能である。例えば２つのブロックのビットを０～$2^{L}-1$の範囲内にある整数として解釈し、対応する暗号文ブロックをそれらの積と定義することにより、固定された数Ｌのキーストリームビットを Ｌ個の平分ビットと組み合わせるようなブロック暗号化システムを考えることができる。このシステムによって、周知のエルガマルの公開キー暗号システムに多少類似した暗号化システムが得られる。不幸なことに、この方法は平文の長さの２倍の暗号文を発生する。

本システムにおける好ましい組み合わせ方法は、準ブロック状の暗号を発生する方法である。古典的な暗号用語では、このアルゴリズムのこの部分は疑似ランダム転置暗号と組み合わされた実行キー暗号とを比較できる。このアイデアは、キーストリームの一部（すなわち発生器の出力）を平文ブロックのバイト（または個々のビット）の疑似ランダム順列を発生する手段として利用することにより、まず中間暗号文ブロックを作成することである。次に中間暗号文ブロックとキーストリームのその後の部分とをＯＲ演算によりビットごとに、またはルックアップテーブルを用いた置換を実行することによりバイトごとに組み合わせる。このような方法は、平文の長さと同じ長さの暗号文本文を発生する。（最終部分ブロックに合わせるため、平文長さがブロックサイズの整数倍になっていない場合

に

は若干異なる取り扱いが必要である。）

明らかな改良方法として、上記疑似ランダム転置方法（順列）と置換方法とを交互に実施することにより、この組み合わせ方法をカスケード状に実行する方法がある。

好ましい組み合わせ方法に関連する性能上の欠点は、必要な発生器の出力の量が増すことにすぎない。しかしながら、ミクスチャー発生器は極めて高速に作動するので、極端に早い暗号化ビットレートを必要とするようなアプリケーションを除けば、大きな問題は生じにくい。更に、最大の可能な安全度を得るためには、重要なことではないが、単一のランダム初期化キーＲで暗号化された平文の最大長さを制限することをアドバイスできる。極めて長い平文は受け入れ可能なサイズの一連のセグメントに単に分解できるので、このことは大きな制約とはならない。

種々の目的を達成するため、キーストリームと平文とを組み合わせるより複雑な方法として、暗号ブロックチェイン接続のような公知の技術の変形例がある。１つの変形例では、まず平文を固定サイズのブロックに分解し、このブロックに付加的タイミング、認証または誤り訂正情報を加えることができる。次に、各平文ブロックをキーストリームの次のブロックと組み合わせる前に、先の暗号文ブロックとＸＯＲ演算する。

ＲＰＫシステムをソフトウェアで実現する際には一度にミクスチャー発生器の８ビット（またはそれ以上）をクロックすることは困難なことではなく、したがって全組み合わせ方法を実行できることに注目することは有効である。この方法は、受け入れ不能な複雑でないハードウェアでも実行できる。

要約すれば、暗号化方法は次のステップを実行する。すなわち、これらステップのすべてはミクスチャー発生器およびその成分を用いて実行される。

まず、ランダム初期化キーＲを発生し、これを使って基底ステートを累乗し、よって暗号文の本文に先行するヘッダー内に含まれる公開キーＱを発生する。

再びＲを使用して公開キーＥを累乗し、最終（内部）発生器の初期化ステート

Ｋを発生する。

ステートＫから開始し、ミクスチャー発生器を作動させ、キーストリーム出力

を得て、このキーストリーム出力と平文Ｐとを組み合わせ、暗号文Ｃの本文を得る。

ここで、Ｒは同じ公開キーを用いて再び同一の平文を暗号化する場合でもＲはランダムに選択されるので、第２暗号文は第１暗号文とランダムに異なることとなり、公開キーＱおよび暗号文本体の双方でも最終（内部）発生器の初期化ステートは異なることとなる。

６．キーストリームと平文との組み合わせ

次に、上記進歩した多数の方法を含む新規な好ましい組み合わせ方法について説明する。次に、平文が８ビットバイトのシーケンスとして表示されるものとし、用語「現在のＣＲＣ値」は開始点から始まり、平文内の特定バイト位置まで続く平文部分に対応する３２ビットのＣＣＩＴＴ周期的冗長性チェック値を意味するものとする。しかしながら、この用語は他のタイプのＣＲＣまたはメッセージダイジェスト計算または本明細書で後に述べるタイプの一般化されたＣＲＣも等しく意味すると解すべきである。更に、バッファの内容として表示される適度に大きい「チャンク」内で組み合わせのために平文を処理することが好ましいと考える。かかる一般的なチャンクのサイズは、２０００～４０００バイトの大きさである。最後に、用語「休止を繰り返しながら進むキーストリーム」とは、１つ以上の成分発生器のクロック制御がステートに従属するように改善されたミクスチャー発生器の出力を意味するものとする。これを行う簡単な方法は、発生器のステージの特定の組みのステートを検出し、ステートがある基準に従う場合、発生器の出力を廃棄する（すなわち別の時間で発生器をクロック制御する）ことである。例えば成分の４つのステージの特定の組がすべて１を含む稼働かを検出し、この場合、この成分を余分な時間でクロック制御することができる。この方法は、キーストリーム発生器の非線形性、従って複雑さを更に増すことがよく知られている。

一般的な組み合わせ方法は次のとおりである。まず現在のチャンクの端部をと

おして平文の現在のＣＲＣ値を計算する。次に、休止を繰り返しながら進むキーストリームの一部を使用して現在のチャンク内のバイトの疑似ランダム順列を発生し、順列データと、休止を繰り返しながら進むキーストリームのその後に続く

バイトとをＸＯＲ演算する。最後に休止を繰り返しながら進むキーストリームを現在のＣＲＣ値に応じたバイト数だけクロック制御し、こうして発生したバイトを廃棄する。廃棄するバイト数は、例えば、現在のＣＲＣ値の単なる低次のバイトの数値で示すことができる。このような最終工程によりチャンクと組み合わせるのに使用されるキーストリーム部分がチャンク前の初期発生器のステートおよび全平文の双方に応じ、よって、あるタイプの暗号ブロックチェイン接続として見ることができるようになる。また、この最終工程は暗号文内の単一ビットの変化、すなわち送信エラーにより、解読された文のうちのその後のチャンク内に平均５０％のエラーのカスケードを生じさせることもできる。

チャンク内でデータを疑似ランダム状に順列する方法は、効率上の要因によって決まることができるように変えることができる。１つの経済的な方法として、チャンクサイズが２５６の倍数でない場合、２５６バイトのブロックより短い端部ブロックが続く可能性のあるチャンクを２５６バイトブロックのシーケンスと見る方法がある。証明するように、１２７の休止を繰り返しながら進むキーストリームバイトを用いてすべての２５６バイトブロックに対して使用すべき１つの疑似ランダムスワップテーブルを発生し、更に、より少ない付加的な数の休止を繰り返しながら進むキーストリームバイトを使用して、必要な場合により短い端部ブロックに対して使用すべき１つのより小さい疑似ランダムスワップテーブルを発生することができる。２５６バイトのブロックのケースに対しては、かかる疑似ランダムスワップテーブルは０～２５５の範囲内の異なる整数の１２８の対（ｉ、ｊ）の組を発生する。スワップテーブルを使用するには、テーブル内の各（ｉ、ｊ）に対しブロック内のバイトｉとｊの位置とを交換するだけでよい。この方法の重要な特徴は、本質的に自己反転可能であること、すなわち同じ順列を２回目に実行すると、元のバイトの順序が再現できるということである。ブロックサイズｎが偶数である場合、かかるスワップテーブルの可能な総数は次の式に

よって示されると指摘することは興味のあることである。

$$\frac{n!}{2^{(n/2)}(n/2)!} = (n-1)(n-3)\ldots(3)(1)$$

サイズｎのスワップテーブルを発生するための、特に簡単なアルゴリズムは、Ｃプログラム言語で書かれた次の一部の文で簡単に記載できる。

```
typedef unsigned char BYTE;
BYTE stut_clock8(void);
#define MODULO    %
#define NOT_EQUAL     !=

void MakeSwapTable(int n, BYTE * table)
{       int index, remaining, i, k;
        BYTE temp;

        for (i = 0; i < n; i++)
          table[i] = i;
      for (k = 0, remaining = n; remaining > 1; remaining = remaining - 2)
      {
         index = k + 1 + ( stut_clock8( ) MODULO (remaining - 1) );
         k = k + 1;
         if (index NOT_EQUAL k)
         {
              temp = table[index];
              table[index] = table[k];
              table[k] = temp;
         }
         k = k + 1;
      }
}
```

上記コードにおいて、関数ＳＴＵＴ＿ｃｌｏｃｋ８（）は、休止を繰り返しながら進むキーストリームの次のバイトを戻す。これが実行された後、ｔａｂｌｅ［］アレイは０～ｎ－１の整数の連続する疑似ランダムペアのシーケンスを含む。（ｎが奇数である場合、最終テーブルエントリーはスワップされないバイト位置を示す。）

計算上のオーバーヘッドの最適な増加量が受け入れ可能であれば、２５６バイトブロックごとに異なる疑似ランダムスワップテーブルを使用する上記方法の、多少複雑な変形例が可能である。いずれのケースでも、各メッセージに対しキーストリームの異なる（更にランダムに選択された）部分が使用されるので、各暗号化されたメッセージに対して使用される実際の順列は異なることを強調するこ

とには意味がある。

最後に、この方法は上記組み合わせ方法の一部を構成するものではないので、有効化および認証化の問題を強調するこの方法の別の特徴について指摘する。暗号方法の終了時には全平文に対するＣＲＣの値を利用できるので、この値を平文に添え、これを暗号化するか、またはこの値の暗号化された変形例を所望する場合、メッセージのヘッダーに挿入することは比較的簡単なことである。送信中にこのメッセージが変わったかどうかを検出するよう、この結果生じた情報を暗号解読中に使用できる。ＣＲＣまたは一般化されたＣＲＣ以外の概略的対策をここで使用することができ、特定の安全条件はリベストＭＤ４アルゴリズムまたはＮＩＳＴ安全ハッシュアルゴリズムのような別の方法を使用できることを示唆できる。

次は、チャンクサイズを（簡略化のため４バイトしかないと考えた好ましい組み合わせ技術の一例である。

平文チャンク「ＡＢＣＤ」（この１６進表示は４１　４２　４３　４４）である。

休止を繰り返しながら進むキーストリーム出力（１６進）：３７　０４　ＦＦ　Ｂ０　５５である。

暗号化：

１．平文チャンクに対するＣＣＩＴＴ　ＣＲＣ３２の値を計算する。この値はＤＢ　１７　２０　Ａ５（１６進表示）に変わる。

２．休止を繰り返しながら進むキーストリームの第１バイトを使用して、疑似ランダムスワップテーブルを発生する（文内のＣ言語フラグメントによって示された方法を適用する）。

ａ）テーブルを０１２３に初期化する。

ｂ）第１の休止を繰り返しながら進むキーストリームバイト３７、モジュロ３は１であるので、テーブル内の要素１および２を順列し、０２１３のテーブルを発生する。

ｃ）この結果生じるスワップテーブルはペア（０、２）および（１、３）を含む。

３．０番目と２番目のバイトをスワップし、次に１番目と３番目のバイトをスワップすることにより、バイトＡＢＣＤを順列し、ＣＤＡＢを発生する。この１６進表示は４３　４４　４１　４２である。これが順列されたチャンクとなる。

４．順列されたチャンクを、その後に続く休止を繰り返しながら進むキーストリームバイトとバイトごとにＸＯＲ演算する。４３と０４のＸＯＲ演算は４７であり、４４とＦＦのＸＯＲ演算はＢＢであり、４１とＢ０のＸＯＲ演算はＦ１であり、４２と５５のＸＯＲ演算は３７であるので、暗号文は（１６進の）バイトシーケンス４７　ＢＢ　Ｆ１　３７から成る。

５．ＣＣＩＴＴ　ＣＲＣ３２の値の最終バイトはＡ５となり、これは１０進の１６５に等しいので、次に次のチャンクを暗号化する前に休止を繰り返しながら進むキーストリームのうちの１６５バイトを発生し、廃棄する。

７．暗号解読

受信した暗号文を解読するため、ユーザーＡは、まずQ^D（ここで、その指数は受信者のプライベートキーＤである）に対応する発生器のステートを計算するため、メッセージヘッダー内に含まれる公開キーＱによって示されたステートを使用する。ＱをＤで累乗するこの方法は、暗号化中にＥをＲで累乗するのに使用される同じ種類の方法を使用して行われる。この結果生じる発生器のステートはＫであると考えられる。その理由は、Ｑは基底ステートa_0からスタートした時間Ｒ後の発生器のステートを示し、時間Ｒ・Ｄ後のステートは先に述べたようにちょうどＫであるからである。多項式表示では、この事実は次のように表示できる。

$$E^R = (X^D)^R = K = (X^R)^D = Q^D$$

このことは、受信者が暗号化のため発生されたランダム初期化キーＲを知る必要なくＫを計算できたことを意味している。次にユーザーＡは、最終初期化ステートＫからスタートしてミクスチャー発生器を作動し（すなわち連続ステートを通過するように発生器をクロック制御し）、暗号化中に実行された組み合わせプロセスを反転（すなわちアンドゥー）するのに必要なキーストリームビットを得

る。ミクスチャー発生器は暗号化および暗号解読の双方のためにステートＫからスタートされるので、キーストリーム出力は双方のケースで同一となる。

暗号化のために使用される組み合わせ方法が、単なる平文とキーストリームとのＸＯＲ演算を実行するとした場合、この結果生じる暗号文と同じキーストリームを再びＸＯＲ演算すれば平文が再現されることになる。先に述べた好ましい組み合わせ方法では、各連続するブロックに対し逆の順序で疑似ランダム転置および置換演算を反転し、平文から暗号文を再現することが容易である。

先に述べた好ましい組み合わせ方法に関する、暗号解読に必要な特定のステップは次のとおりである。

１．プライベートキーを使用し、平文のヘッダーに含まれる公開キーＱを累乗し、最終初期化キーＫを計算する。これを行うための方法は、暗号化中に公開キーをランダム初期化キーで累乗するのに使用した方法と同じである。次に、ミクスチャー発生器のステートはＫで与えられる。

２．暗号文本体の各ブロックに対し、ミクスチャー発生器を作動させ、キーストリーム出力の一部を得てこれを使用し、疑似ランダム順列テーブルを発生する。

３．次にミクスチャージェネレータを作動し、別のキー出力を得てこれと暗号文ブロックとをビットごとにＸＯＲ演算するか、またはルックアップテーブルを使用してバイトごとにこれらを組み合わせ、中間文ブロックを発生する。このステップは暗号化中に実行された置換プロセスを逆に進むものである。

４．先に作成された順列テーブルによって定義された疑似ランダム順列を適用する。このステップは暗号化中に実行された転置方法を逆に進むもので、元の平文のブロックを発生する。

先に述べた好ましい組み合わせ方法では、反転の若干より複雑な方法が必要である。発生器を初期化するのにとられるステップは、単に組み合わされた暗号文の解読のためのステップと同じである。しかしながら、組み合わせ方法をアンドゥーする方法では、まずチャンクごとに休止を繰り返しながら進むキーストリームの等価的部分を使用し暗号化方法において平文に対して適用される順列を反転するのに必要な方法に対応する代表的チャンクの代表的疑似ランダム順列を発生

するステップを実行する。次に、現在の暗号文チャンクと休止を繰り返しながら

進むキーストリームのその後の連続するバイトとをＸＯＲ演算する。これにより、平文の、解読されているが疑似ランダム順列バージョンが発生する。第３に、代表的チャンクに適用された同じ順列を平文の順列バージョンに適用し、平文を再現する。最後に、現在のチャンクの終了部までの解読文の現在のＣＲＣ値を計算し、現在のＣＲＣ値に応じたバイト数だけ休止を繰り返しながら進むキーストリームをクロック制御する。チャンクの各２５６バイトブロックのバイトの順序を再び決めるのに、疑似ランダムスワップテーブルを用いて疑似ランダム順列を適用した先の例では、キーストリームと暗号文とをＸＯＲ演算する前に同じスワップテーブルが発生される。次に、その結果生じる、解読されているがまだ順列状態にある平文に対して、自己反転性であるスワップテーブルを使用し、平文を再現する。

次は、好ましい組み合わせ技術の先の例に対応する好ましい分離技術の一例である。

暗号文４７　ＢＢ　Ｆ１　３７の暗号解読

１．正しい暗号解読キー（プライベートキー）が入手可能であると仮定すれば、休止を繰り返しながら進むキーストリームバイトのシーケンスは、暗号化に使用されたシーケンス３７　０４　ＦＦ　Ｂ０　５５と同一となる。

２．第１の休止を繰り返しながら進むキーストリームバイトを用いて暗号化方法と同じように疑似ランダムスワップテーブルを発生する。

３．スワッピング前に暗号文と休止を繰り返しながら進むキーストリームの連続するバイトとをＸＯＲ演算する。４７　ＸＯＲ　０４＝４３、　ＢＢ　ＸＯＲ　ＦＦ＝４４、Ｆ１　ＸＯＲ　Ｂ０＝４１、　３７　ＸＯＲ　５５＝４２となる。従って、中間暗号文は４３　４４　４１　４２となる。

４．まず中間暗号文の０番目のバイトと２番目のバイトをスワッピング化、次に１番目のバイトと３番目のバイトをスワッピングする（４１　４２　４３　４４）ことによりスワップテーブルを適用する。

５．この結果は４１　４２　４３　４４となり、これはＡＳＣＩＩストリング

ＡＢＣＤ、すなわち正確に暗号解読された平文の１６進表示である。

６．この点までの平文に対するＣＲＣ３２１を計算する。以前と同じように、最終バイトはＡ５であり、以前と同じように次のチャンクを暗号解読する前に休止を繰り返しながら進むキーストリームの次の１６５バイトを発生し、廃棄する。

８．ハードウェアの実現

本システムは、ソフトウェアでの実現が容易であるが、顕著な利点の１つとして、極めて高速の特殊用ハードウェアでも実現できるということが挙げられる。超大規模集積回路技術は極めて急速に進歩しているので、特定の実現例の詳細はすぐに時代遅れとなってしまう。しかしながら、かかる実現の相対的な容易性または困難性および達成可能な速度に展望を与えるような既製の構成部品が存在してる。例えばカナダの会社であるニューブリッジマイクロシステムズ社によって製造されているＣＡ３４Ｃ１６８キー管理プロセッサのようなＧＦ［2^n］のような累乗を実行する特殊チップも存在している。このチップは１６メガまで作動し、フィールドＧＦ［2^{593}］のような累乗を行うＴＴＬコンパチＣＭＯＳデバイスである。このチップのスループットは毎秒３００Ｋビットである。このフィールドは、本システムに対しては必ずしも理想的でないが、これらの仕様は、公開キー、オープンキーおよび最終発生器初期化キーを計算できるレートのあるアイデアを提供するものである。上記会社は２０Ｋビット／秒で真のランダムビットストリームを発生するＲＢＧ１２１０ランダムビット発生器を製造しており、かかるデバイスは本発明で必要なランダム初期化キーＲを発生するのに適している。極めて高速で作動できる極長シフトレジスタおよびディスクリートのロジックゲートも既製品として入手でき、カスタムチップとなるように容易に集積化でき、またはフィールドプログラマブルゲートアレイとして実現できる。

第４図は、暗号化装置のハードウェアによる実現例を示しており、一方、第５図は暗号解読方法のハードウェアによる実現例を示しており、いずれもハードウェアで先に述べた機能を実行している。

９．サインおよび認証

先の方法の主要で、かつ重要な変形例は、受信し、解読した平文が特定のソース（すなわちユーザーB）から発信されたものであり、偽造されたものでないことを暗号メッセージの受信者（本明細書の用語例ではユーザーA）が確認できるようにすることにある。この条件は、オリジナルなものを証明し、他の誰かがサインを偽造できないように、何人もサインと公に入手可能な情報とを比較できるような性質を備えたサインをメッセージに添えることができるようにすることである。この条件は、新しいメッセージまたは偽のメッセージのためのサインを発生するよう、先のメッセージのサインを使用することができないようにしなければならないことも意味していると解すべきである。従って、かかるデジタルサインはメッセージに依存したものであることが重要である。

ここで、公開キー暗号システムの基礎となる、まだ明瞭に述べられていない仮定とは、（アドレスおよびそれらの公開キーのリストを含む）公開ファイルが不正な変更に対して安全でなければならないことを明示することである。このようなケースでない場合、侵入者は他人の公開キーを自分のキーとを交換し、不正が発覚するまで犠牲者の安全性を危うくすることができる。かかる不正な扱いに対するかかる公開ファイルの安全性は、通常はパスワードシステムまたはコールバック方法およびときどきは物理的手段によって得られている。

ここで、サインコミュニケーションを望む個人が登録した適当な情報を保持する安全な公共のサインアーカイブ（文書館）が存在し、このアーカイブは誰でも調査のために利用できるが、正当な加入者以外の者が変える恐れがないように、安全になっていると仮定する。更に、このアーカイブの安全性は、加入者が自分のファイルに付加的サイン情報を添付できるが、システム管理者が変更の記録と追跡をできるようにする適当な監査トレールから離れることなく、現在の情報を変更したり削除することができないと仮定する。また、かかる予防手段は従来の種々のサンプルサインの周りにめぐらした予防手段から過度に異なるものではないことに言及したい。

公共サインアーカイブは暗号システム用の公開キー情報を含むアーカイブと同じようにできるが、２つのファイルは異なるファンクションおよび恐らく異なる

法的ステータスを有することに留意したい。変更およびアクセスのコストと頻度も異なる構造と異なる管理条件を有することができ、これら２つの公にアクセス可能なファイルを分離することが望ましいことが示唆される。

バックグラウンドとして、メッセージのためのＣＲＣ（周期冗長性チェック）の値の概念を要約する。ＣＲＣ値はファイルおよび通信の完全性のインディケータとして共通に使用されており、種々の国際的規格（例えばＣＣＩＴＴ規格）が存在している。１つのメッセージのＣＲＣ値は、一般に１６または３２ビット長であり、メッセージ文内のわずかな変化、ひずみまたは誤りが完全に異なるＣＲＣ値を生じさせるようにメッセージから計算される。この計算方法は、本質的には特定ＣＲＣ生成多項式によりメッセージ多項式（その係数はメッセージのビットである）を分割するのに（ハードウェアまたはソフトウェアで実現された）シフトレジスタ発生器を使用するものである。このＣＲＣ値は、ＣＲＣ生成多項式の剰余モジュロの係数を示す。３２ビットのＣＣＩＴＴ規格の場合では生成多項式は次のとおりである。

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

本認証方法はＣＲＣ概念を利用するものである。特に、本明細書に述べた例のミクスチャー（ジェフ）発生器の場合、メッセージＭに対しC_M＝（C_{Mm}、C_{Mt}、C_{Mb}）を定義でき、これら３つの成分の各々はメッセージ文を対応する生成多項式ｐ（ｘ）で割ることにより得られた発生器のステートを示す。割り算を実行するのにシフトレジスタを利用する方法は他の文献に良好に記載されているので、この方法については本明細書では説明しない。C_Mはｐ（ｘ）の倍数までのメッセージ自体にほぼ等価的な値を示す。

このようなバックグラウンドにおいて、安全な認証方法は次のとおりである。通信システムへの各加入者は、加入者に固有で、かつ公共サインアーカイブまたは他のメッセージ認証機関に登録された認証パスワードＰの排他的知識を有すると仮定する。公共サインアーカイブすなわち認証機関は、本発明の要旨である公開キー暗号システムを参照しながら先に定義された対応する公開キーE_Sと共に

、自分のプライベートキーDSを所有する。ユーザーBがユーザーAに送信するメッセージMにサインしたい場合、ユーザーBは一般化されたＣＲＣ値CMを計算し、自分の認証パスワードPBにCMを添え、公共サインアーカイブの公開キーESを使用してペア（PB、CM）を暗号化することにより、サインSMを形成する。加入者は次にメッセージにこのサインSMを添える。

メッセージの受信者または第三者がサインSMの正当性を証明したい場合、受信者は実際のメッセージに対する一般化されたＣＲＣ値C'M を計算し、これをサインSMおよびユーザーBを識別する名前または他の情報と共にこれを認証のための公共サインアーカイブすなわち認証機関へ送る。公共サインアーカイブまたは認証機関はプライベートキーDSを使用してそのサインを解読し、その内部に含まれる一般化されたＣＲＣ値とC'M の値とを比較し、含まれていたパスワードとユーザーBに対し登録された認証パスワードとを比較する。これらの双方が一致すれば、公共サインアーカイブはサインをユーザーBによるメッセージMの正当なサインとしてサインを有効にする。

メッセージの真のサイン者しかサインSMを発生できないことは、上記記載より理解できよう。そのようにサインをするには、ユーザーBの認証パスワードとメッセージの一般化されたＣＲＣ値の双方の知識が必要であるからである。暗号化された一般的ＣＲＣ値は、これに対応するメッセージの１つの一致するので、別のメッセージにサインしようとするため有効なサインを偽造する試みは成功しない。この方法の利点は、メッセージをサインするたびに公共認証アーカイブに付加的情報を挿入する必要がないことである。

次に、公開キー認証システムの別の好ましい実施例について説明する。ユーザーBがユーザーAへ送るメッセージMにサインしたい場合、乱数SMm、SMtおよびSMbを発生し、成分発生器ごとにCM ＋SM およびVM ＝X^{S_M}ｍｏｄ　ｐ（ｘ）を計算する。次にユーザーBは公共サインアーカイブに自分の名前でペア（CM

＋S_M、V_M）を登録し、メッセージヘッダーにS_Mを添えることによりメッセージにサインをする。既に公共サインアーカイブにV_mが登録済みであれば、ユーザーＢは固有のV_mが決定されるまで新しいS_mおよび対応するV_mを計算してこのプロセスを繰り返す。（すなわち公共サインアーカイブには、まだ未登録である。）

上記方法が正当なサインを保証するため、最初にメッセージを所有し、公共サインアーカイブに検査を依頼できる者が真のメッセージに対するＣＲＣ値C'_Mを

計算し、S_Mを加え、その結果が公共サインアーカイブ内に集められた値と一致するかどうか証明することができるように監視する。更に誰もが$V_M = x^{S_M}$

ｍｏｄ　ｐ（ｘ）を計算し、これが公共サインアーカイブ内の値と一致するかどうか実証することも可能である。しかしながら、本発明の基礎となる暗号化方法は（後述するように）適度に安全であると仮定すれば、ユーザー以外の者がこれら条件に合致するサインS_Mを判断することはできない。他の認証方法で共通するように、同じＣＲＣ値と共に偽のメッセージを発生する可能性は、特定のメッセージ構造、すなわちプロトコルを主張することによって妨げることができるが、本方法が３つ以上の異なる多項式を利用することにより、かかる予防策はほとんど不要となる。

１０．成分発生器としての乗法的合同発生器

いわゆる乗法的合同発生器（ＭＣＧ）、すなわちレーマー発生器は、疑似乱数発生器としてコンピュータシステムで広く使用されている。このタイプの発生器の最も簡単な変形例では、式$x_n = c\,x_{n-1}$（ｍｏｄ　ｑ）を使用して番号のシーケンスを発生する。ここで、ｑは素数であり、ｃは２とｃが単位の素原子根（ｐｒｉｍｉｔｉｖｅ　ｎｏｏｔ　ｏｆ　ｕｎｉｔｙ）となるように選択された（ｑ－１）との間の一定の整数である。開始値すなわちシードx_0は任意に選択される。例えば、ｑは$2^{31}-1$となるように選択されることが多く、この$2^{31}-1$は適当なメルセンヌ素数であり、ｃは整数５２４２８７として選択できる。この結果生じる１と（ｑ－１）との間の整数のシーケンスは、２者の二進表示が全部０

または全部１となる場合を除き、すべて３１ビットの整数の順列となる期間（ｑ－１）を有する。

これらシーケンスは計算が迅速かつ容易であり、妥当な長さとなるという魅力的な性質を有するが、（非線形にシャッフルされていない場合）疑似乱数発生器として使用した場合、統計的な性質がよくないということが長く知られており、Ｄ・ヌース（D. Knuth）は暗号化技術においてキーストリーム発生器としての不適性に関する詳細な分析を発表している。しかしながら、これらの弱点は、これまで述べ、高度な非線形の構造を有するタイプのミクスチャー発生器における成分発生器としての有効性を必ずしも損なうものではない。

法ｑが2^n-1の形態をしたメルセンヌ素数となるようにＭＣＧを選択すると仮定すれば、発生器の出力はｎビットのブロックで発生する。これらブロックは

下位ビットでスタートするビットストリームとして見ることができる。ＭＣＧを特定ビット数だけクロック制御すること、すなわち進めることは、必要なブロックを得るのに適当な数の整数の累乗と乗算モジュロｑを実施し、次にブロック内の正しいビット位置を選択することによって達成される。従って、このタイプの成分発生器に対しては、整数の乗算モジュロ2^n-1は多項式の乗算モジュロｐ（ｘ）と置き換わる。この方法は、これと共に大きな整数に対する演算を実行しなければならないが、特にｑがメルセンヌ素数である場合、このように演算を適当に効率的に実行する方法が存在している。

ミキサー発生器としてＭＣＧを使用することは、発生器内のいくつかの固定されたビット位置の内容によって示された二進ステートを使用し、残りを廃棄することにより（すなわち出力が選択される発生器とｎ倍のレートでＭＣＧをクロック制御することにより）、またはＭＣＧビットストリーム出力内の連続するビットのグループを使用することにより、達成できる。後者の方法の一例は、ＭＣＧをミキサーとして使用し、他の８個の発生器（それらの構造はここでは無関係である）のうちから選択する図１に示された例に類似している。この選択を行うのにＭＣＧから生じるビットの全ストリームを一度に３ビットずつ使用できる。

１１．暗号化技術の安全性（セキュリティ）

次にプライベートキーから公開キーへの変換によって得られる安全レベルおよび発生器のキーストリーム出力と平文との単純なＸＯＲ組み合わせから得られる暗号文の性質の双方について一般的に説明する。

プライベートキーに対する、いわゆる「選択された平文への侵入」の条件に関して、ここに提案するシステムの安全レベルは、対応する公開キーが知られ、侵入者が暗号システムの完全な知識を有し、この知識を用いて、選択されたプライベートキーに対応する公開キーを発生できる場合のプライベートキーを発見する上での計算上の困難性に直接対応している。例えば第２図に示されるような発生器の構造を仮定した場合、３つの成分ＭＬＳＲＧの各々の出力をＧＦ（2^P）として知られる次数2^Pの有限場の要素として数学的に見ることができる。各メッセージに対し、異なるランダム初期化キーＲが選択されるので、与えられたプライベートキーに対応する公開キーを発生するのに発生器を進める作動は、ＧＦ（2^P）を累乗することに数学的に等価的であるとみなすことができ、公開キーからプライベートキーを探す反転問題はＧＦ（2^P）に対する対数を計算することに数学的に等価的である。従って、ここに提案されたシステムのこの部分の計算上の安全性のレベルは、ＧＦ（2^P）に対する対数を計算する困難性に匹敵する。１９７０年の終わりに、これを行うための最良の公知のアルゴリズムは、次数$2^{P/2}$での演算を必要としていたが、この分野のより最近の進歩により、現在知の最良の方法を使用するには次数$2^{c\cdot\sqrt[3]{p\cdot\log^2 p}}$での演算しか必要でないことが判っている（ここで、ｃは約１．４または１．５に経験的に概算された小さい定数である）。ｐ＝１２７となるように（１、３０、１２７）ＭＬＳＲＧを使用する場合、これら２つの量を比較すると、第１の場合の約６３の指数と第２の場合の約２６または２７との差異が判る。このことは、最初は不可能であったＧＦ（2^{127}）の対数を計算することは、現在では適度に困難なことにすぎず、最新のメインフレームコンピュータで数時間を要するにすぎないことを意味している。第２図に示されたジェフ構造で長さ８７、８９および１２７の３つのＭＬＳＲＧを使用した、本明細書の最初で示した小さい例に関して、これら数字は計算

上の適度なレベルが得られることを意味している。

８９、１２７および５２１のＭＬＳＲＧ長さを備え、同じジェフ発生器構造を使用する示唆されたより大きい例では、ここに提案する公開キーシステムはパソコンでも容易に実現できるが、その計算上の安全性の例はより高いものである。長さ５２１の最長の発生器だけを検討すると、上記数字はＧＦ（2^{521}）に対する対数を計算するのに必要な演算数は、最適に近いと考えられる現在知られている最良のアルゴリズムを使用した場合、約2^{50}の大きさとなる。現在のコンピュータの大きさが数桁改善されると仮定しても、これら状況では提案された公開キーシステムは計算上安全である。すなわち計算リソースと無関係に、すべての利用可能な情報から未知のプライベートキーを計算することは不可能である。更に、暗号化および解読に必要な計算力を最適に増加し、付加的キー長さの結果として公開キーファイルに過度の負担をかけることなく、更に大きい成分発生器を使用することができ、この結果、システムの安全性を任意のレベルまで高めることができる。

シフトレジスタ発生器の代わりに乗法的合同発生器を使用することにより、離散的対数の問題の計算上の困難性が増し、よって暗号化方法の安全性が高まる傾向がある。これはＧＰ（2^{P}）に対してでなく、ｑが素数である場ＧＦ（ｑ）に対して対数を計算しなければならないからであり、この場合に対する現在知られている最良のアルゴリズムは効率が悪く、法ｑがメルセンヌ素数$2^{P}-1$である場合、次数$2^{c\sqrt{p\log p}}$の演算が必要である。例えばこの演算は、ｑ＝１２７である場合、大まかに言って約2^{40}～10^{12}回の演算となり、これはＧＦ（2^{P}）の場合よりも数千倍多い。

次に、キーストリーム発生器および先に述べた組み合わせ方法に対する選択された平文の侵入への観点から、システムの安全性について検討する。このタイプの侵入は、暗号解読者がすべての公開キーにアクセスし、解読者が平文と暗号文のメッセージの対応する対を発生するのに使用できるキーストリーム発生器（本例ではミクスチャー発生器）へ直接アクセスすることを含む完全な暗号システム

を入手している場合の侵入である。このような状況は、暗号解読者が発生器の任意の初期ステートから開始してキーストリーム出力から選択した長さの任意の数のサブシーケンスを検討できることを意味している。ここで、ミクスチャー発生器の時間長さは極めて長い（説明したジェフ構造の最初のものに対してでも2^{30} 3）ことに留意されたい。

キーストリームのうちの多数のかかる部分（サーチフラグメント）を発生し、これらの各々と未知の暗号文とのスライド相関化を実行することにより、暗号解読者は統計的解析により検出できるオーバーラップを発見しようとする。検出可能なオーバーラップの可能性はメッセージの長さと発生器が作動できる速度に依存するが、確率論的解析はオーバーラップする可能性は極めて小さいと示す。例えば発生器が毎秒１０００ギガビット（毎秒2^{40}ビット）でクロック制御でき、平文長さが平均１ギガビット（2^{30}ビット）であり、わずか2^{10}ビット（１キロビット）長さのサーチフラグメントを使用するスライド相関器により、サーチフラグメントとのオーバーラップを瞬間的（すなわち０時間ないに）有効に検出できると仮定しても、より小さいジェフタイプの発生器の場合、特定の暗号文を探すのに予想される時間は2^{240}秒もの大きさとなる。

確率論的解析も同じ仮定をした場合、ランダムに選択された初期化キーに対応するメッセージに対するオーバーラップの可能性は無視できるものであり、よってこの方法（いわゆる共通誕生日問題）に基づく公知の平文への侵入も徒労に終わることを示している。更に、未知の暗号文に対応する平文の部分が暗号解読者により知られている（または推定できる）と仮定した場合でも、かかる既知の部分の長さが発生器の複雑さすなわち図示されたジェフタイプの発生器よりも小型のものでも５８１９３の複雑さを越えない限り、（実行キー暗号化器の解答と同じように）キーストリームを拡張し、平文の残りの部分を解くことができない。このような離間した偶然性は単一ランダム初期化キーにより暗号化すべき平部分の最大長さを制限し、必要な場合、より長いメッセージをセグメント状に分けることによって解決できるが、その結果生じる性能上の欠点に鑑み、安全性の向上を評価すべきである。

解読者が出力キーストリームと成分発生器との間の相関性を発見しようとする、より簡単な形態の相関性への侵入は、数学的な文献に記載されいるが、成分発生器の時間が極めて長く、その自動相関化およびクロス相関化の性質が優れているので、本システムでは効率的でない。

１２．小さい例

暗号化用には有効ではないが、明確にするため、ここに提案するシステムの作動を示すため、小さい例を含める。この例は、第２図に示されたジェフ構造のＭＬＳＲＧ成分を使用するものである。第３図には個々の発生器が示されており、そのステージ数は所定ステージに対応するｘの級数を示す。

これら３つの発生器のための生成多項式ｐ（ｘ）はそれぞれ次のとおりである。

$$1+x+x^2,\quad 1+x+x^3,\quad 1+x^3+x^5$$

これら３つの発生器の全出力ストリーム（すなわちフル時間）は、次のとおりである。

ﾐｷｻｰ：１０１

頂部：１００１０１

底部：００１０００１０１１１０１１０００１１１１１００１１０１

表1

ミキサー		頂部		底部	
ステート	$1x$	ステート	$1xx^2$	ステート	$1xx^2x^3x^4$
01	10	001	100	00100	10000
10	01	100	010	00010	01000
11	11	010	001	00001	00100
		101	110	10000	00010
		110	011	01000	00001
		111	111	10100	10010
		011	101	01010	01001
				10101	10110
				11010	01011
				11101	10111
				01110	11001
				10111	11110
				11011	01111
				01101	10101
				00110	11000
				00011	01100
				10001	00110
				11000	00011
				11100	10011
				11110	11011
				11111	11111
				01111	11101
				00111	11100
				10011	01110
				11001	00111
				01100	10001
				10110	11010
				01011	01101
				00101	10100
				10010	01010
				01001	00101

上記表1は、これら発生器に対するステートの全シーケンスおよびそれに対応する多項式の定数（すなわちxの適当な級数に合わせるよう番号をつけ直したステージを備えたステート）を示している。しかしながら、関係する発生器の大き

さは実際的な意味で表１の計算を不可能にするものであり、ここには単なる図解のために含めたものであることを強調したい。表の列をソートすると、対数モジュロ生成多項式の表が有効に得られる。

ここで、初期ステートは次のように示される。

$$a_{m_0} = \begin{pmatrix}0\\1\end{pmatrix},\quad a_{b_0} = \begin{pmatrix}0\\0\\1\end{pmatrix},\quad a_{b_0} = \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}$$

第３図に示されたステージ番号を検討すると、これらステートの各々は次の多項式に対応することが判る。

$$1 = 1x^0 + \sum_{j=1}^{n-1} 0x^j.$$

これら３つの成分発生器の各々に対し、ｘの二進級数に対応する多項式係数は、下記の表２に示されるように容易に計算される（モジュロｐ（ｘ））。これら級数に対応するステートはこれらビットを適当に回転するだけで（すなわち番号をつけ直すだけで）得られることを強調したい。

表２

級数　k	ミキサー x^k		頭部 x^k		底部 x^k	
	ステート	$1x$	ステート	$1xx^2$	ステート	$1xx^2x^3x^4$
$2^0 = 1$	10	01	100	010	00010	01000
$2^1 = 2$	11	11	010	001	00001	00100
$2^2 = 4$			110	011	01000	00001
$2^3 = 8$					11010	01011
$2^4 = 16$					10001	00110

Ｄ＝（３、６、２４）なるプライベートキーを選択すると、表２を広範に使用することにより、次のように対応する公開キーを計算する。

ａ）D_m＝３（二進で１１）であるので、まず多項式 x^2 に対応するステート１１をミキサー発生器にロードし、次にこのミキサー発生器を１回クロックし、

ｘを乗算することにより$x^3 = x^2 x^1$を計算すると、ステート０１が得られる。これは次の式を与える。

$$E_n = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

ｂ）D_t＝６（二進で１１０）であるので、まず多項式x^4に対応するステート１１０（多項式の係数０１１）を頂部発生器にロードし、次にこれを２回クロックし、x^2を乗算することにより$x^6 = x^4 x^2$を計算すると、ステート０１１が得られる。すなわちこれにより次の式が得られる。

$$E_t = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

ｃ）D_b＝２４（二進で１１０００）であるので、$x^{24} = x^{16} \cdot x^8$を計算すればよい。これは第２の因数$x^8$が２つ以上の０でない係数を備えた多項式に対応するので、先のケースよりも若干複雑である。表２から$x^8 = 0. 1 + 1.$

$x + 0 x^2 + 1. x^3 + 1. x^4$（すなわち多項式係数は０１０１１）であるので、$x^{16}$に対応するステート１０００１を３回発生器にロードし、このクロックを１回、３回および４回それぞれクロックし、ｘ，x^3およびx^4を乗算し（その理由は、これらはx^8における０でない係数を備えたｘの係数であるからである）、次に対応する係数モジュロ２を加える。この結果生じるこれら３つのステートは次のとおりとなる。

１１０００，１１１１０，１１１１１

これら対応する係数モジュロ２を加えると、１１００１の最終ステートが得られる。すなわち、これにより次の式が得られる。

$$E_b = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

他のあるユーザーが文字ＡＡ（その二進数によるＡＳＣＩＩ表示は０１０００００１　０１０００００１である）の平文を暗号化することによりメッセージを送りたいと仮定する。発信者は、まずランダム初期化キーＲを発生する。これを行う種々の手段は可能であり、例えば雑音ダイオードを利用する方法がある。

ここで、ＲはＲ＝（２、３、７）として発生されたものと仮定する。

発信者の最初の作業はＱを計算することである。この作業はＤからＥを計算するように行われ、以前と同じように表２を活用する。

ｄ）Q_mはステート１１として表のx^2ラインから直接呼び出すことができる。

ｅ）$x^3 = x^2 x$を計算することによりQ_tを得る。x^2に対応する頂部発生器のステートは０１０であり、これら内容を発生器にロードし、発生器を１回クロックしてｘを乗算すると、ステート１０１が得られる。

ｆ）Q_bを計算するため、表２を使用して底部発生器に対する$x^7 = x^4 x^2 x$を計算する。これら級数の最後の２つは、１つの０でない係数しか含んでいないので、底部発生器に０１０００（x^4に対応するステート）を

ロードし、発生器を２回クロックし、最後に１回クロックすることは容易である。この結果得られるステートは１０１０１となる。

よって、メッセージヘッダーは次のようにＱを含む（付加的メッセージ固有の情報も含むことができる）。

$$Q_m = \begin{pmatrix}1\\1\end{pmatrix},\ Q_t = \begin{pmatrix}1\\0\\1\end{pmatrix},\ Q_b = \begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix}$$

次のステップはＫを計算することである。これは、同様な乗算方法により行うが、今回は公開キーＥの成分に対応する多項式をＲで示される級数で累乗することにより行う。

ｇ）まずE_mに対応する多項式を級数$R_m=2$で累乗することによってK_mを得る。本例ではE_mは０次の多項式$1=1\,x^0+\sum_{j=1}^{n-1}0\,x^j$であるので、任意の級数に累乗される１は１となるのと同じように、計算は不要である。従って、K_mはE_mと同じであり、ステート０１に対応する。このような状況は実際には決して予想できないものである。このような状況は、D_mをミキサー発生器の時間長さに等しい３と選択することによって生じる。システムを実現する際、ＤまたはＲに対する明らかに良好でない選択をすることは、簡単に拒否される。

ｈ）次に、E_tを級数$R_t=3$で累乗する。これを計算するにはｘでなくてE_tの二進級数をリストアップする表２に類似する表を作成する必要がある。本例のためには$E_i^3=E_i^2\cdot E_i$であるので、E_i^2を計算するだけでよい。E_iは多項式$1+x^2$に対応するステート０１１であるので、頂部発生器にこのステートをロードし、これを２回クロックし、１００を得て、次にこれら値のモジュロ２の対応する係数を加え、E_i^2に対応するステート１１１を得る。次に、発生器を再び使用してこの値にE_tを乗算する。この乗算が発生器に１１１をロードし、これを２回クロックして００１を得て、これらのモジュロ２の係数を加え、最後にK_tに対する１１０を得ることによって行う。

ｉ）K_bを計算するため、E_bを級数$R_b=7$で累乗する。また、E_b^4およびE_b^2を得るには表２に類似する表を作成する必要があるので、$E_b^7=E_b^4\cdot E_b^2\cdot E_b$を計算する。$E_b=11001=x^2+x^3+x^4$を得るので、$E_b\times^2=10110$、$E_b\times^3=01011$および$E_b\times^4=00101$（これらは発生器をクロックすることによって得られる）のモジュロ２の合計としてE_b^8を得るので、これによりx^3+x^4に対応する１１０００が得られる。これを２乗すると、１００００としてのE_b^8が得られ、最後に０１１０１としてのK_bが得られる。

従って、ステートＫは次の式で示される。

$$K_m=\begin{pmatrix}0\\1\end{pmatrix},\ K_t=\begin{pmatrix}1\\1\\0\end{pmatrix},\ K_b=\begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}$$

ｊ）これらステートからスタートする３つの発生器からの出力ストリームは次のとおりとなる。

ﾐｷｻｰ：１０１１０１１０１１０１１０１１０１....

頂部：０１１１００１０１１１００１０１１１００１....

底部：１０１１０００１１１１００１１０１００１０００１０１０１１..

ｋ）この結果得られるミクスチャー（キーストリーム）の最初の１６ビットは次のようになる。

００１１００１１１１１００００１....

１）このストリームと平文との排他的ＯＲを計算すると次の暗号文が得られる。

０１１１００１０１０１００００

ｍ）この暗号化方法はＱの成分をプライベートキーＤによって示される級数で累乗することによってＫを計算することに始まる。この累乗方法は既に上記ステップｇ）、ｈ）およびｉ）で示された方法に完全に類似する方法である。簡単

に述べれば、

$$K_m = Q_m^{D_m} = Q_m^3 = \begin{pmatrix}0\\1\end{pmatrix},\quad K^t = Q_t^{D_t} = Q_t^6 = Q_t^4 \cdot Q_t^2$$

およびステート１１１および０１１にそれぞれ対応する最後の２つの因数を得るので、

$$K_t = \begin{pmatrix}1\\1\\0\end{pmatrix}$$

となる。最後に、$K_b = Q_b^{D_b} = Q_b^{24} = Q_b^{16} \cdot Q_b^8$ を計算し、それぞれのステート

１１１１０および０１１００に対応する後者の２つの因数を計算する。これにより次の結果が得られる。

$$K_b = \begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}$$

ｎ）（予想するように）ステートＫはメッセージの発信者によって計算されるステートと同じであるので、このステートからミクスチャー発生器をスタートすることにより、上記ステップｊ）およびｋ）に示されているのと同じキーストリーム出力が発生し、このキーストリーム出力は暗号文とＸＯＲ演算され、平文を再現できる。

１３．ランダム化およびキー管理の問題

本方法は、現在のシステムと比較するとかなり多い総数のキービットを使用する。例えば米国データ暗号化規格（ＤＥＳ）は、キーのために５６ビットを使用しているが、上記例で使用したジェフタイプの発生器は、成分発生器の長さの合計に等しい８７＋８９＋１２７＝３０３のキービット、または８９＋１２７＋５

２１＝７３７のキービットを使用する。これら長いキーは高いレベルの安全性を提供するが、特殊なキー管理技術の利点が得られるようにするには、これらの長さは充分に長い。

まず、より素朴な形態の暗号分析侵入から保護するため、容易に思い出すか、またはシステム的に発生されるパターンよりもすべての暗号化キーを最良にランダムに選択する。真のランダムビットストリームを発生するための周知のハードウェア手段、例えばノイズ発生ダイオードが存在している。別の方法としては、生物学的測定方法を使用することである。今日では、実質的にすべてのパソコンでマイクロ秒分解能のハードウェアが存在しているので、この例は連続する非同期的な、人により発生される事象、例えばキーストロークの間の時間間隔を広くすることである。かかる期間の長さの下位の桁は許容可能なランダムな性質を有する。いずれの場合でも、かかるキーをシステマティックに、または繰り返して使用することは、システムの安全性にシビアに妥協することとなるので、できるだけ真にランダムに、本発明におけるランダム初期化キーＲを選択する試みが重要である。本発明は、多次元（例えば２次元）のコンピュータ入力装置、例えばペン、描画パッド、マウスまたは他のポインティングデバイスまたはタッチスクリーンとともに、別の生物学的測定技術を使用することが考えられる。ユーザーにランダムなパターンを描くことが求められ、一方発生されたパターンの種々の可能性のある属性を使用して適度にランダムな入力を得ることができる。例えば、マウスが利用できる場合、マウスの特定時間におけるマウスの座標を表示する数字の下位ビットを適当なものとすることができる。これと異なり、特定時間におけるマウスの速度または特定タイプのマウスの事象、またはマウスがトレースするパラメータ曲線の空間的性質（例えば曲率）を使用することができる。

好ましい実施例としては、この目的のためにコンピュータディスプレイスクリーンにディスプレイされるウィンドーのエリア内で多少ランダムにマウスポインタを動かす（すなわちそれを振ったり、それで描く）ことをユーザーに要求できる。連続する時間におけるコンピュータの作動環境によって検出されるマウスポインタの位置のｘおよびｙ座標を適当な下図のマウスの運動が生じるまで１６ビットの２進数の連続するペアとして記録できる。これらポイントの、例えば最初

の２５％と最後の２５％を十分にランダムでないものとして廃棄でき、他の残りのすべての１６ビット座標値の下位の４ビットを抽出し、連結し、所望の乱数を形成できる。

ハードウェアおよびソフトウェアの急な変化により測定中の属性のランダム性が破壊されないように保証するための注意が必要である。例えばマイクロソフトのウィンドウズが作動する環境では、外部事情、例えばマウスまたはキーボードの事象に利用できるタイミング分解能はわずか５０ミリ秒であるので、第２事象のタイミングは極めて非ランダムとなり得る。更に、かかる侵入は安全性への深刻な脅威となり得るので、システムのタイミング情報またはマウス事象処理とインターフェースする試みを保護しなければならない。

コンピュータシステムで一般に使用されているほとんどの疑似乱数発生器はこれらのニーズには適当ではないが、本明細書に述べたミクスチャー発生器のキーストリーム出力は優れたランダムな性質を有し、ここで検討している妥協方法を提供するものである。特に、真にランダムなソースから各成分発生器内に適当な数のステートを初期化し、発生器を短い（すなわち１０００クロックサイクルの）間、作動または進める場合、その結果生じる最終発生器のステートは真にランダムなステートからは統計学的に区別できないものとなる。この方法をキーハッシング（混信）方法と称す。ここに説明した発生器の複雑性が高いことより、このことはこれまで説明した他の手段、例えばいわゆるカウンターモードでＤＥＳチップまたはアルゴリズムを使用するようなことに対する妥当な代替案が提供される。

暗号化キーの記憶および管理は解決しなければならないが、公開キーシステムは従来のプライベートキーシステムよりもその安全性に対する要因に依存する率は本来的に低い。コンピュータまたはデータ記憶システム内の何らかの場所にプライベートキーを記憶する場合、物理的安全性が重要な問題となる。あるアプリケーションでは暗号化機器またはコンピュータの電磁気放射を考慮しなければならない。ポータブルなメディア、例えば磁気的または光学的にエンコードされたカードにコンパクトに記憶することは可能であるが、人の記憶だけにしか存在しないようなデータ（例えばパスワード）からキーを構成するか、またはこれより

容易に発生できるようにコストまたは他の要因が支配できる従来のアルファニューメリック記号は１つの文字につきわずか５～６ビットの情報しか提供せず、代表的なパスワードは８～１０文字以下に制限されているので、このようにわずか５０～６０のキービットしか供給できない。

本発明は、パスワードから得られるキービットによりミクスチャー発生器の成分発生器の限られた数のステージを初期化し、上記方法をまね、ランダムキーをシミュレートするように何時間もの間発生器を作動または進めることを考えるものである。かかるシステムは、暗号解読によるキークラスターの攻撃を受け易いが、初期化、すなわちハッシング段階において使用されるクロックサイクルの数を拡張し、（発生器の急速な進行を禁止し、よってトライアルキーを発生できるレートを制限するよう）中断を繰り返しながら進むような非線形を導入することにより、安全性を高めることができる。

産業上の利用性

本発明の暗号化システムは、真の公開キーシステムから得られる利点を備えた安全な通信が求められるようなほとんどの領域で用途がある。非制限的例としては次のものがある。

（１）インターネットのような公共的ネットワークを通してクレジットカードの番号すなわち認証を含む個人または財務情報を安全に転送すること。

（２）インターネットを含む現在のコンピュータネットワークまたは交換回線を通して安全な音声通信の送信をし、かかる通信のプライバシーを保証すること。

この用途では、シークレットキーに先に接触または予めアレンジする必要なく、リアルタイムでデジタル化された、および／または圧縮された音声データを暗号化できる。

（３）インターネットを含むコンピュータネットワークまたは公衆交換回線のいずれかを通した電子メールまたはファクシミリ通信のプライバシーを保証すること。

利点

・公知の暗号解析が困難なこと

本アルゴリズムの暗号解析に成功することの困難度を定量的に評価できる。アプリケーションの予定する分野に応じてシステムパラメータを直接的に選択することにより、この困難度を任意のレベルに合わせることが可能である。

・高速性

本アルゴリズムは、ソフトウェアで実現するにせよ、またはハードウェアで実現するにせよ、次の作業をできるだけ迅速に達成可能とするものである。

ａ）任意に選択されたプライベートキーから公開キーを発生すること。

ｂ）任意の平文ビットストリームを暗号化すること。

ｃ）暗号化された暗号文を解読すること。

・高い安全性

本システムは最新の暗号規格および方法に関し、高度に複雑な最新の暗号解読のおそれに対し、極めて高い安全性を提供できる。

・暗号文の最小長さ

送信時の非効率性を防止するため、本システムは長さが平文の長さにほぼ等しい暗号文を発生する。

・非決定論的であること

同じ公開キーを用いて２回以上同じ平文を暗号化することがシステムに求められている場合でも、この結果生じる各暗号文は、コードブックの収集を防止し、他の暗号解読の攻撃を失敗させるため、非システマティックな態様で、他の暗号文と異なる。

・実現が簡単で、かつ効率的であること

このシステムを実現するのに必要な不可欠な計算は、計算機器に対する要求を最小にしながらハードウェアまたはソフトウェアで達成することができる。これにより、埋め込みシステム、注文すなわち専用ハードウェア、またはスマートカードのみならず、広範に入手できるプロセッサ上で走るソフトウェアでの実現を容易にするものである。

【図１】

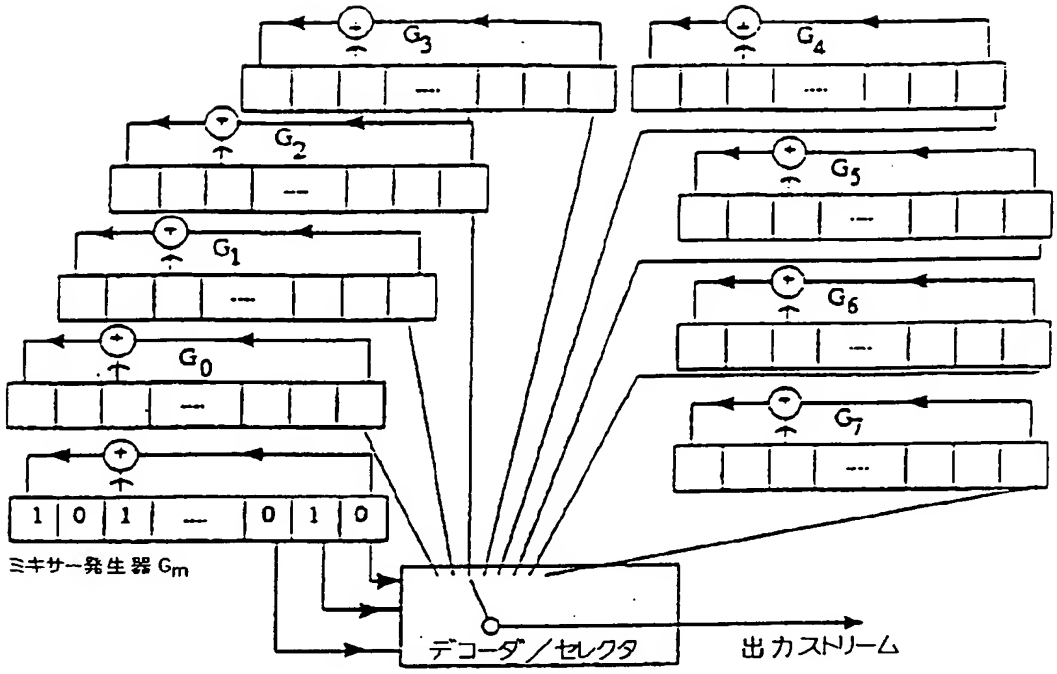


FIG 1

【図２】

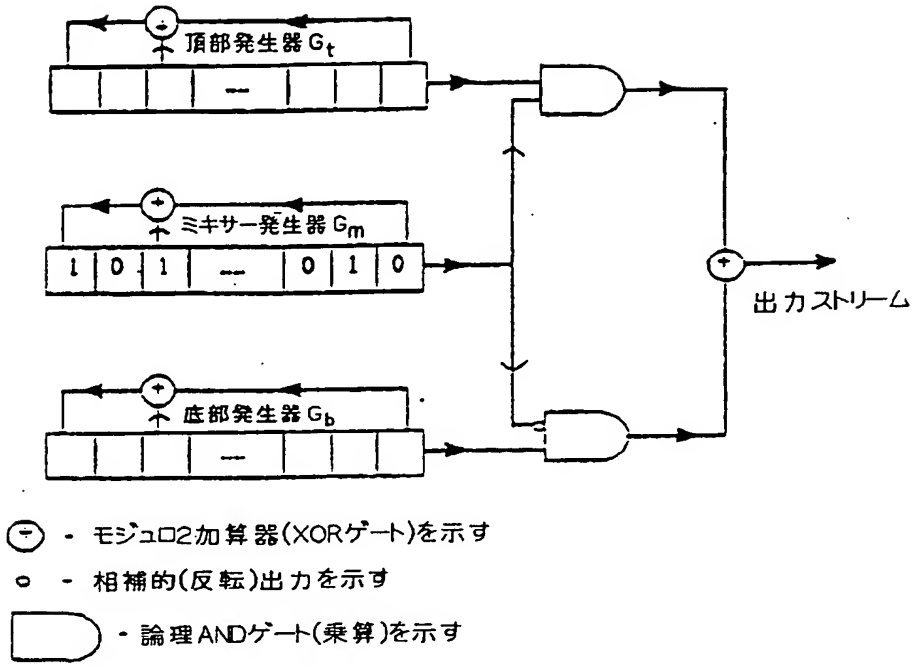

頂部発生器 G_t
ミキサー発生器 G_m
1 0 1 --- 0 1 0
底部発生器 G_b
出力ストリーム
⊕ - モジュロ2加算器(XORゲート)を示す
○ - 相補的(反転)出力を示す
- 論理ANDゲート(乗算)を示す

FIG 2

【図３】

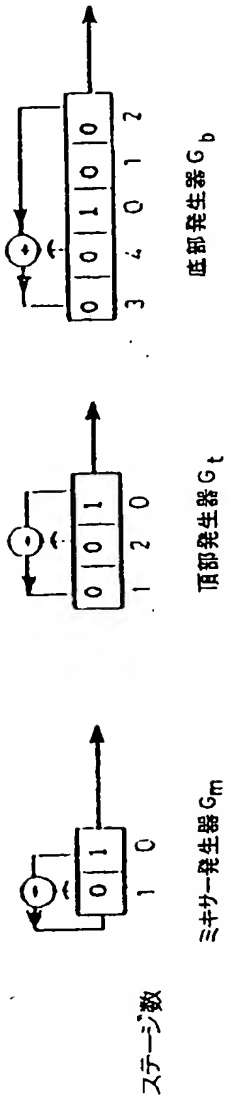


FIG 3

【図４】

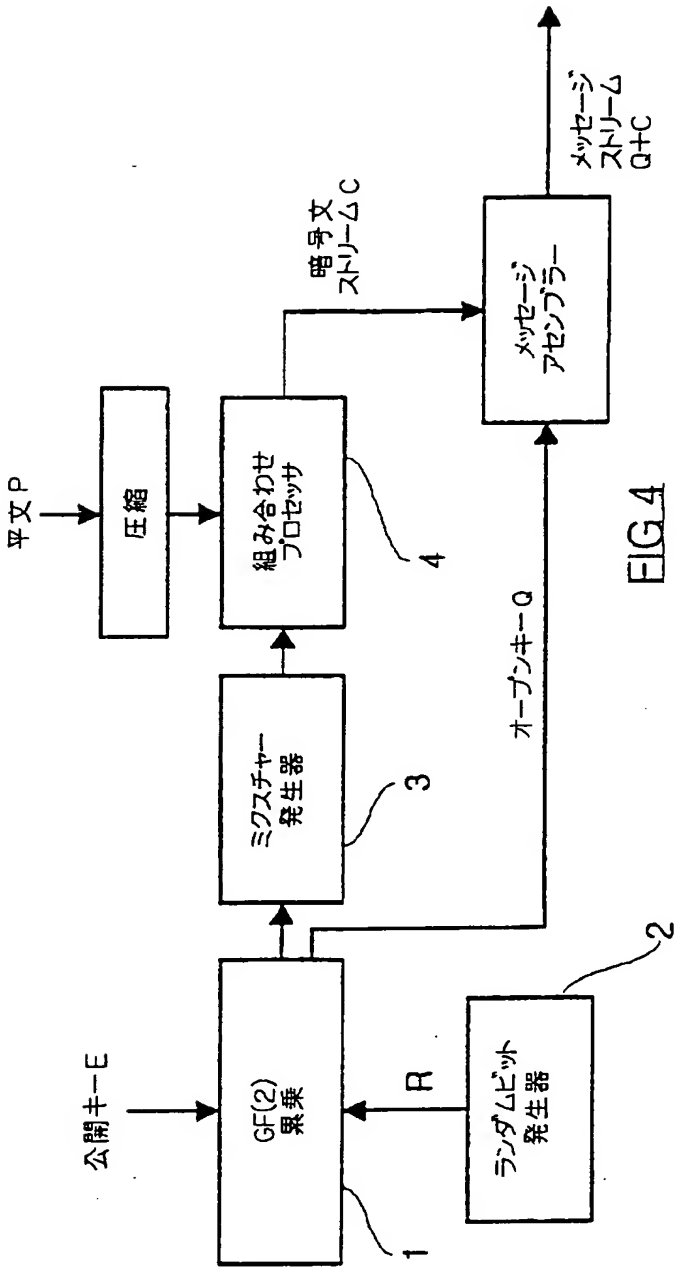

公開キーE
GF(2)
累乗
1
R
ランダムビット
発生器
2
ミクスチャー
発生器
3
組み合わせ
プロセッサ
4
圧縮
平文P
暗号文
ストリームC
メッセージ
アセンブラー
メッセージ
ストリーム
Q+C
オープンキーQ

FIG 4

【図５】

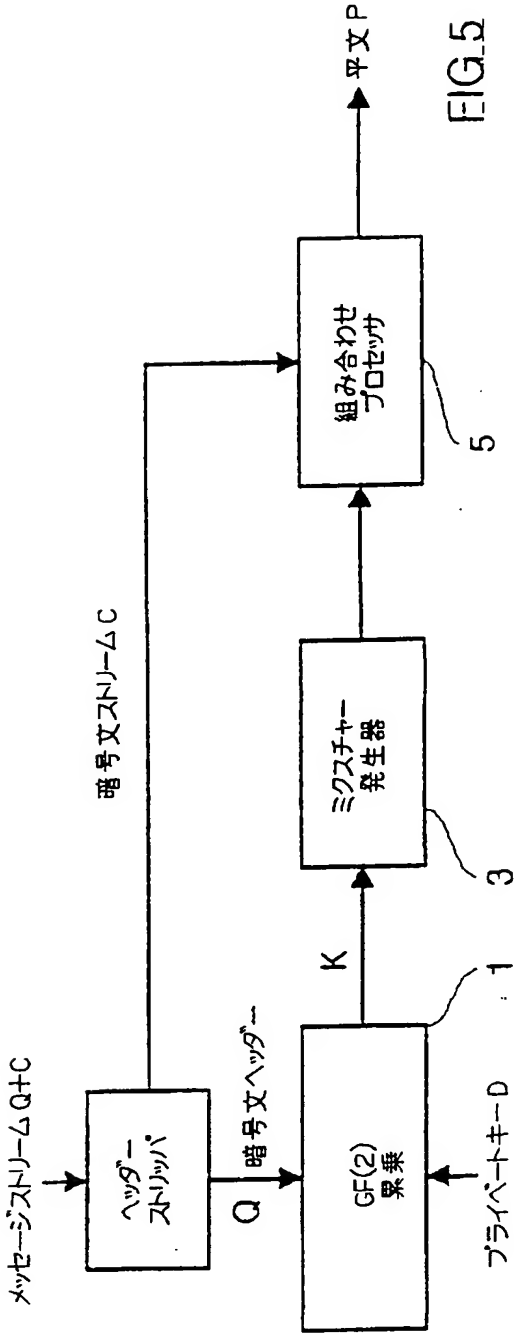

メッセージストリームQ+C
ヘッダー ストリッパ
Q
暗号文ヘッダー
暗号文ストリームC
GF(2) 累乗
プライベートキーD
K
1
ミクスチャー 発生器
3
組み合わせ プロセッサ
5
平文P

FIG.5

【手続補正書】特許法第１８４条の８

【提出日】１９９５年６月２７日

【補正内容】

２．前記ミクスチャー発生器が一組（ｎ）の最大期間線形シフトレジスタまたは乗法的合同発生器を備え、組内の１つの発生器が前記キーストリームシリアル出力を発生するようクロック制御されるたびに、組のうちの残り（ｎ－１）の発生器のうちの１つの出力を疑似ランダムに選択するようになっている、請求項１記載の公開キー暗号システム。

１５．公開キー暗号システムで使用するのに適したミクスチャー発生器であって、

一組（ｎ）の最大期間線形シフトレジスタまたは乗法的合同発生器と、

ミクスチャー発生器の出力を発生するよう、前記発生器のｎ－１個のうちの１つから出力を選択するための手段と、

ｎ番目の発生器のうちの複数（ｍ）の最後のステージの出力をデコードするためのデコード手段とを備え、

該デコード手段の出力が、使用する特定の発生器の出力の選択を決定するよう、前記選択手段を制御するミクスチャー発生器。

【国際調査報告】
INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ 94/00136

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl.[6] H04L 9/30, 9/32, 9/06, 9/24, 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC H04L 9/30, 9/32, 9/06, 9/24, 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU: IPC as above

Electronic data base consulted during the international search (name of data base, and where practicable, search terms used)
DERWENT: shift registers
JAPIO: shift registers

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	US,A, 4165444 (GORDON) 21 August 1979 (21.08.79) whole document	15,16
A	EP,A, 325238 (YEDA RESEARCH AND DEVELOPMENT COMPANY LIMITED) 26 July 1989 (26.07.89) whole document	9

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
23 February 1995 (23.02.95)

Date of mailing of the international search report
6 Mar 1995 (06.03.95)

Name and mailing address of the ISA/AU

AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION
PO BOX 200
WODEN ACT 2606
AUSTRALIA

Facsimile No. 06 2853929

Authorized officer

R FINZI

Telephone No. (06) 2832213

Form PCT/ISA/210 (continuation of first sheet (2)) (July 1992) copgid

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ 94/00136

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international search report has not established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-7,9,15,16, directed to a mixture generator or the use of a mixture generator in a public key encryption/decryption/authentication system.
2. Claim 10, directed ot a random number generator.
3. Claim 8, directed to a public key authentication system using a pseudorandom number generator.
4. Claims 11-14, directed to methods of combining a datastream with a keystream to form an encrypted stream.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically

claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-7,9,15,16

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family membe:

International application No.
PCT/NZ 94/00136

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	4165444	GB	1597218				
EP	325238	AT	99818	AU	631111	CA	1331642
		DE	68911935	ES	2049764	JP	1309088
		US	4933970				

フロントページの続き

(51) Int.Cl.6	識別記号	庁内整理番号	FI		
H04L 9/32		9570－5J	H04L 9/00		675B

(31)優先権主張番号 260712
(32)優先日 1994年6月9日
(33)優先権主張国 ニュー・ジーランド（NZ）
(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, MW, SD, SZ), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN

【要約の続き】
る。本発明は特殊用途のハードウェアまたは汎用プロセッサ用のソフトウェアで実現できる。